COURBES ELLIPTIQUES

par

François Brunault

Résumé. — Ce texte est constitué des notes d'un cours de M2 donné à l'ÉNS Lyon au second semestre 2008/2009. On trouvera des exercices à la fin de chaque chapitre. La référence pour ce cours est [**3**], qui contient de nombreux autres exercices.

Table des matières

1. Fonctions elliptiques

Définition 1.1. — On appelle *réseau* de $\mathbf{C}$ tout ensemble de la forme $\Lambda = \{m\omega_1 + n\omega_2; m, n \in \mathbf{Z}\}$, où (ω_1, ω_2) est une base de $\mathbf{C}$ comme espace vectoriel sur $\mathbf{R}$. L'ensemble $\{t_1\omega_1 + t_2\omega_2; 0 \leq t_1, t_2 \leq 1\}$ est un *domaine fondamental* de Λ (cf. figure 1).

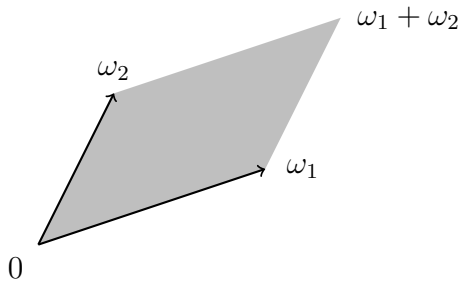


FIG. 1. Un domaine fondamental

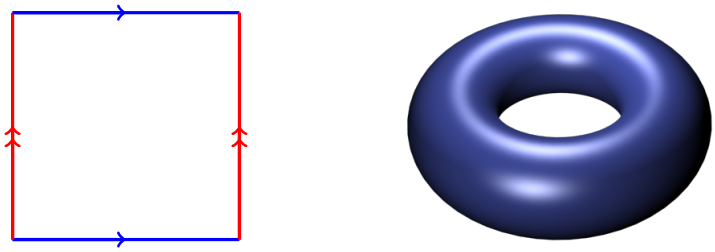


FIG. 2. Une courbe elliptique sur $\mathbf{C}$

De manière équivalente, un réseau est un sous-groupe discret Λ de $\mathbf{C}$ tel que $\mathbf{C}/\Lambda$ est compact (pour la topologie naturelle sur le quotient).

Si Λ est un réseau de $\mathbf{C}$, le quotient $\mathbf{C}/\Lambda$ est un *tore complexe* de dimension 1. Un tel tore est homéomorphe à $(\mathbf{R}/\mathbf{Z})^2$ et s'obtient à partir d'un domaine fondamental en identifiant les côtés opposés (cf. figure 2).

Si $\alpha\Lambda \subset \Lambda'$ avec $\alpha \in \mathbf{C}^*$, alors la multiplication par α induit un *morphisme* de tores complexes $\mathbf{C}/\Lambda \to \mathbf{C}/\Lambda'$. C'est un isomorphisme si et seulement si $\alpha\Lambda = \Lambda'$. On prendra garde au fait que les tores complexes sont tous homéomorphes, mais ne sont pas tous isomorphes !

Définition 1.2. — Soit Λ un réseau de $\mathbf{C}$. Une *fonction elliptique* pour Λ est une fonction f méromorphe sur $\mathbf{C}$ qui est Λ-périodique, *i. e.* vérifie $f(z+\lambda) = f(z)$ pour tout $z \in \mathbf{C}$ et $\lambda \in \Lambda$ où l'égalité a un sens. On note $\mathbf{C}(\Lambda)$ l'ensemble des fonctions elliptiques pour Λ.

L'ensemble des pôles d'une fonction elliptique f est invariant par translation par Λ et définit donc une partie de $\mathbf{C}/\Lambda$. C'est une partie discrète

et fermée de $\mathbf{C}/\Lambda$, donc finie car $\mathbf{C}/\Lambda$ est compact. De même, l'ensemble des zéros de f ($\neq 0$) est une partie finie de $\mathbf{C}/\Lambda$. On en déduit que $\mathbf{C}(\Lambda)$ est un corps.

Pour tout $f \in \mathbf{C}(\Lambda)^*$ et $P \in \mathbf{C}/\Lambda$, l'*ordre d'annulation* de f en P est un entier relatif bien défini, qui est noté $\mathrm{ord}_P(f)$. De même, le résidu de f en P est bien défini. Un *diviseur* sur $\mathbf{C}/\Lambda$ est une somme formelle finie à coefficients dans $\mathbf{Z}$ de points de $\mathbf{C}/\Lambda$, c'est-à-dire un élément de l'algèbre de groupe $\mathbf{Z}[\mathbf{C}/\Lambda]$. Le *degré* d'un diviseur $D = \sum_{i=1}^k n_i[P_i]$ est $\sum_{i=1}^k n_i$. Le *diviseur de* $f \in \mathbf{C}(\Lambda)^*$ est

$$\mathrm{div}\, f = \sum_{P \in \mathbf{C}/\Lambda} \mathrm{ord}_P(f) \cdot [P] \in \mathbf{Z}[\mathbf{C}/\Lambda].$$

Un tel diviseur est dit *principal*.

Proposition 1.3. — *Pour tout $f \in \mathbf{C}(\Lambda)^*$, on a les formules*

$$\sum_{P \in \mathbf{C}/\Lambda} \mathrm{Res}_P(f) = 0 \tag{1}$$

$$\sum_{P \in \mathbf{C}/\Lambda} \mathrm{ord}_P(f) = 0 \tag{2}$$

$$\sum_{P \in \mathbf{C}/\Lambda} \mathrm{ord}_P(f) \cdot P = 0. \tag{3}$$

Démonstration. — Posons $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$. Soit $a \in \mathbf{C}$ tel que f n'a ni zéro ni pôle sur la frontière ∂M de $M = \{a + t_1\omega_1 + t_2\omega_2; 0 \leq t_1, t_2 \leq 1\}$. Par le théorème des résidus $\sum_{P \in \mathbf{C}/\Lambda} \mathrm{Res}_P(f) = \frac{1}{2\pi i} \int_{\partial M} f(z)dz$ et cette intégrale est nulle par périodicité de f, d'où (1). En appliquant (1) à la fonction elliptique f'/f, on obtient (2). Enfin, utilisons le théorème des résidus pour la fonction $zf'(z)/f(z)$, il vient $\sum_{P \in M} \mathrm{ord}_P(f) \cdot P = \frac{1}{2\pi i} \int_{\partial M} zf'(z)/f(z)dz$. Par un changement de variables on a

$$\int_{a+\omega_1}^{a+\omega_1+\omega_2} \frac{zf'(z)}{f(z)}dz = \int_a^{a+\omega_2} \frac{zf'(z)}{f(z)}dz + \omega_1 \int_a^{a+\omega_2} \frac{f'(z)}{f(z)}dz$$

En reparamétrant, la dernière intégrale vaut $\int_\gamma du/u$ où γ est un chemin fermé évitant 0, et appartient donc à $2\pi i\mathbf{Z}$. On en déduit $\sum_{P \in M} \mathrm{ord}_P(f) \cdot P \in \Lambda$, ce qui entraîne (3). □

Corollaire 1.4. — *Une fonction elliptique non constante possède au moins deux pôles, comptés avec multiplicité dans* $\mathbf{C}/\Lambda$.

Démonstration. — Si $f \in \mathbf{C}(\Lambda)$ n'a pas de pôle, alors f est holomorphe et bornée, donc constante. Si $f \in \mathbf{C}(\Lambda)^*$ n'a qu'un pôle et que ce pôle est simple, cela contredit la proposition 1.3(1). □

Pour construire une fonction elliptique, on part de la fonction $1/z^2$ qui a un pôle double en 0, et on la moyenne sous l'action de Λ.

Définition 1.5. — La fonction $\wp$ de Weierstraß est donnée par

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - \{0\}} \Big(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \Big) \qquad (z \in \mathbf{C}, z \notin \Lambda).$$

Pour $z \in \mathbf{C} - \Lambda$ fixé, cette série converge absolument car le terme général est $O(1/|\lambda|^3)$. La fonction $\wp$ possède un pôle double en les points de Λ et est holomorphe ailleurs.

Lemme 1.6. — *La fonction* $\wp$ *est une fonction elliptique.*

Démonstration. — Soit $\mu \in \Lambda$, $\mu \neq 0$. On a

$$\begin{aligned} \wp(z+\mu) &= \frac{1}{(z+\mu)^2} + \sum_{\lambda \neq 0} \Big(\frac{1}{(z+\lambda+\mu)^2} - \frac{1}{\lambda^2} \Big) \\ &= \frac{1}{(z+\mu)^2} + \sum_{\lambda \neq \mu} \Big(\frac{1}{(z+\lambda)^2} - \frac{1}{(\lambda-\mu)^2} \Big) = \wp(z) + C \end{aligned}$$

avec $C = \sum_{\lambda \neq 0, \mu} (1/\lambda^2 - 1/(\lambda-\mu)^2)$. Le changement de variables $\lambda' = \mu - \lambda$ montre que $C = 0$. □

Remarque 1.7. — Pour tout entier $k \geq 3$, l'expression $\sum_{\lambda \in \Lambda} 1/(z+\lambda)^k$ définit également une fonction elliptique, qui coïncide à un facteur près avec la dérivée $(k-2)$-ième de $\wp$. Remarquons également que $\wp$ est paire et $\wp'$ est impaire.

Pour tout entier pair $k \geq 4$, posons $G_k = \sum_{\lambda \in \Lambda - \{0\}} 1/\lambda^k$.

Théorème 1.8. — *On a l'identité* $(\wp')^2 = 4\wp^3 - 60G_4\wp - 140G_6$.

Démonstration. — Le développement de Laurent de $\wp(z)$ en $z = 0$ est $\wp(z) = 1/z^2 + az^2 + bz^4 + O(z^6)$. Comme $\wp''(z) = 6\sum_{\lambda\in\Lambda} 1/(z+\lambda)^4$, il vient

$$\wp''(z) = \frac{6}{z^4} + 2a + 12bz^2 + O(z^4) = \frac{6}{z^4} + 6G_4 + O(z^2)$$

d'où $a = 3G_4$. On trouve de même $b = 5G_6$. On calcule alors

$$\wp'(z)^2 = \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + O(z^2)$$
$$\wp(z)^3 = \frac{1}{z^6} + \frac{9G_4}{z^2} + 15G_6 + O(z^2)$$

On en déduit que la fonction elliptique $(\wp')^2 - 4\wp^3 + 60G_4\wp$ n'a pas de pôle. Elle est constante d'après le corollaire 1.4, et vaut $-140G_6$ en 0. □

Lemme 1.9. — *Si $z_0 \notin \Lambda$, on a* $\operatorname{div}(\wp(z) - \wp(z_0)) = [z_0] + [-z_0] - 2[0]$.

Démonstration. — La fonction $\wp(z) - \wp(z_0)$ possède un seul pôle (double en $z = 0$), et s'annule en $z = z_0$. D'après la proposition 1.3(2), son diviseur est de la forme $[z_0] + [z_1] - 2[0]$, et 1.3(3) entraîne $z_1 = -z_0$. □

Théorème 1.10. — *Le corps $\mathbf{C}(\Lambda)$ est engendré par $\wp$ et $\wp'$.*

Démonstration. — Nous allons montrer plus précisément que toute fonction elliptique $f \in \mathbf{C}(\Lambda)$ s'écrit de manière unique $f = g + h\wp'$ avec $g, h \in \mathbf{C}(\wp)$. L'unicité résulte de considérations de parité ($\wp'$ est impaire). Pour l'existence, la décomposition de f en somme de fonctions paire et impaire montre qu'il suffit de montrer que toute fonction elliptique paire est dans $\mathbf{C}(\wp)$. Soit $f \in \mathbf{C}(\Lambda)^*$ paire. Alors $\operatorname{ord}_0(f) \in 2\mathbf{Z}$, mais $f(z+\omega)$ est également paire si $\omega \in \frac{1}{2}\Lambda$, d'où $\operatorname{ord}_\omega(f) \in 2\mathbf{Z}$. Ainsi le diviseur de f se met sous la forme

$$\operatorname{div} f = \sum_{i=1}^{k} n_i([z_i] + [-z_i])$$

avec $n_i \in \mathbf{Z}$ et $[z_i] \in \mathbf{C}/\Lambda$. D'après la proposition 1.3(2) on a $\sum_{i=1}^k n_i = 0$. En posant $g(z) = \prod_i (\wp(z) - \wp(z_i))^{n_i}$, le produit étant pris sur les $z_i \notin \Lambda$, on a $\operatorname{div} g = \operatorname{div} f$ grâce au lemme 1.9 puis $f/g \in \mathbf{C}^*$ grâce au corollaire 1.4, d'où $f \in \mathbf{C}(\wp)$. □

Rappelons que la multiplication de $\mathbf{Z}[\mathbf{C}/\Lambda]$ est donnée par $[P]\cdot[Q]=[P+Q]$. Notons I_Λ l'idéal de $\mathbf{Z}[\mathbf{C}/\Lambda]$ formé des diviseurs de degré 0.

Proposition 1.11. — *Soit $D=\sum_{i=1}^k n_i\cdot[z_i]$ un diviseur sur $\mathbf{C}/\Lambda$. Les conditions suivantes sont équivalentes :*

(1) *D est principal.*
(2) *On a $\sum_{i=1}^k n_i=0$ et $\sum_{i=1}^k n_i\cdot z_i=0$ dans $\mathbf{C}/\Lambda$.*
(3) *On a $D\in I_\Lambda^2$.*

Démonstration. — D'après la proposition 1.3, on a (1) $\Rightarrow$ (2). Montrons (2) $\Rightarrow$ (3). Par hypothèse $D=\sum_{i=1}^k n_i\cdot([z_i]-[0])$. Puisque

$$[P+Q]-[P]-[Q]+[0]=([P]-[0])([Q]-[0])\in I_\Lambda^2,$$

l'application qui à $P\in\mathbf{C}/\Lambda$ associe la classe de $[P]-[0]$ dans I_Λ/I_Λ^2 est un morphisme de groupes. Donc $D\equiv[\sum_i n_i\cdot z_i]-[0]\equiv 0 \pmod{I_\Lambda^2}$.

Supposons (3). Comme I_Λ est engendré par les diviseurs $[P]-[0]$, le groupe I_Λ^2 est engendré par les diviseurs de la forme $D=[P+Q]-[P]-[Q]+[0]$. Il suffit de montrer qu'un tel D est principal. Si $P=0$ ou $Q=0$, c'est évident. Sinon, soit $R\in\mathbf{C}/\Lambda$ tel que $2R=Q$ et $P+R\neq 0$. Alors

$$f(z)=\frac{\wp(z-R)-\wp(P+R)}{(\wp(z)-\wp(P))(\wp(z-R)-\wp(R))}$$

vérifie $\operatorname{div} f=D$. □

Définition 1.12. — Le *groupe de Picard* $\operatorname{Pic}(\mathbf{C}/\Lambda)$ est le quotient de $\mathbf{Z}[\mathbf{C}/\Lambda]$ par le sous-groupe des diviseurs principaux.

Soit $\operatorname{Pic}^0(\mathbf{C}/\Lambda)$ l'image de I_Λ dans $\operatorname{Pic}(\mathbf{C}/\Lambda)$. Le groupe $\operatorname{Pic}^0(\mathbf{C}/\Lambda)$ est l'analogue pour les courbes elliptiques du groupe des classes d'idéaux d'un corps de nombres.

***Théorème 1.13* (Abel-Jacobi)**. — *L'application qui à $P\in\mathbf{C}/\Lambda$ associe la classe de $[P]-[0]$ dans $\operatorname{Pic}^0(\mathbf{C}/\Lambda)$ est un isomorphisme de groupes.*

Démonstration. — L'application somme $\sum_i n_i\cdot[z_i]\mapsto\sum_i n_i\cdot z_i$ induit un isomorphisme $\operatorname{Pic}^0(\mathbf{C}/\Lambda)\xrightarrow{\cong}\mathbf{C}/\Lambda$, dont l'inverse est $P\mapsto[P]-[0]$. □

Remarque 1.14. — D'après 1.11, on a aussi $\mathrm{Pic}^0(\mathbf{C}/\Lambda) \cong I_\Lambda/I_\Lambda^2$.

Le *plan projectif complexe* $\mathbf{P}^2(\mathbf{C})$ est le quotient de $\mathbf{C}^3 - \{0\}$ par la relation d'équivalence $(x, y, z) \sim \lambda(x, y, z)$ pour tout $\lambda \in \mathbf{C}^*$. On note $(x : y : z)$ la classe de (x, y, z) dans $\mathbf{P}^2(\mathbf{C})$. On considérera $\mathbf{C}^2$ inclus dans $\mathbf{P}^2(\mathbf{C})$ au moyen de $(x, y) \mapsto (x : y : 1)$.

Proposition 1.15. — *L'application*

$$\phi : \mathbf{C}/\Lambda \to \mathbf{P}^2(\mathbf{C})$$
$$z \mapsto \begin{cases} (\wp(z), \wp'(z)) & si\ z \neq 0 \\ (0 : 1 : 0) & si\ z = 0 \end{cases}$$

est injective. Son image est $\phi(\mathbf{C}/\Lambda) : y^2 z = 4x^3 - 60G_4 x z^2 - 140G_6 z^3$.

Démonstration. — Soit E la partie de $\mathbf{P}^2(\mathbf{C})$ définie par l'équation ci-dessus. On a $\phi(\mathbf{C}/\Lambda) \subset E$ par le théorème 1.8. Si $(x : y : 0) \in E$ alors $x = 0$ et $(x : y : 0) = (0 : 1 : 0) = \phi(0)$. Supposons $(x, y) \in E$. La fonction elliptique $\wp(z) - x$ possède un pôle en $z = 0$ et d'après la proposition 1.3(2), il existe $z_0 \in \mathbf{C} - \Lambda$ tel que $\wp(z_0) = x$. Alors $\phi(z_0) = (x, \pm y)$ et donc $\phi(\pm z_0) = (x, y)$. Enfin, l'injectivité de ϕ résulte du lemme 1.9. □

Proposition 1.16. — *Le polynôme* $4x^3 - 60G_4 x - 140G_6$ *est à racines simples.*

Démonstration. — Puisque $\wp'$ est impaire, on a $\wp'(\omega) = 0$ pour tout $\omega \in \frac{1}{2}\Lambda - \Lambda$, ce qui entraîne avec le théorème 1.8 que le polynôme ci-dessus s'annule en les trois valeurs distinctes $\wp(\frac{\omega_1}{2})$, $\wp(\frac{\omega_2}{2})$ et $\wp(\frac{\omega_1+\omega_2}{2})$. □

Voici une première définition des courbes elliptiques.

Définition 1.17. — Soit k un corps de caractéristique $\neq 2, 3$. Une *courbe elliptique sur* k est une équation E de la forme $y^2 = x^3 + ax + b$ avec $a, b \in k$ tels que $\Delta := 4a^3 + 27b^2 \neq 0$. Si k' est une extension de k, on note $E(k') = \{(x, y) \in k'^2 \text{ vérifiant } E\} \cup \{(0 : 1 : 0)\}$.

Nous verrons au chapitre 3 que $E(k')$ est muni d'une structure de groupe. D'autre part, toute courbe elliptique sur $\mathbf{C}$ est paramétrée par un tore complexe, comme ci-dessus. Voici une manière de l'expliquer :

dans la proposition 1.15, on peut reconstituer le réseau Λ à partir de l'image de ϕ, au moyen de la forme différentielle $dz = \phi^*(dx/y)$.

Exercices. — Soit $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ un réseau de $\mathbf{C}$.

1.1. Déterminer le diviseur de la fonction elliptique $\wp'$.

1.2. Exprimer $\wp''$ comme un polyôme en $\wp$. Montrer plus généralement que toute fonction elliptique holomorphe sur $\mathbf{C} - \Lambda$ est un polynôme en $\wp$ et $\wp'$, et même en $\wp$ si la fonction est paire.

1.3. Montrer que $\wp''(\frac{\omega_1}{2}) = 2(\wp(\frac{\omega_1}{2}) - \wp(\frac{\omega_2}{2}))(\wp(\frac{\omega_1}{2}) - \wp(\frac{\omega_1+\omega_2}{2}))$ et donner des formules analogues pour $\wp''(\frac{\omega_2}{2})$ et $\wp''(\frac{\omega_1+\omega_2}{2})$.

1.4. Montrer que $G_8 = \frac{3}{7}G_4^2$. Montrer plus généralement, pour tout entier pair $k \geq 4$, que G_k est un polynôme à coefficients rationnels en G_4 et G_6.

1.5. À quelle condition sur la fraction rationnelle $f \in \mathbf{C}(z)$ l'expression $f_\Lambda(z) = \sum_{\lambda\in\Lambda} f(z+\lambda)$ définit-elle une fonction elliptique ? Montrer que si f est paire (resp. impaire) alors f_Λ est paire (resp. impaire).

1.6. La fonction ζ de Weierstrass.

(a) Montrer qu'il n'existe pas de fonction elliptique f telle que $f' = \wp$.

(b) Montrer qu'il existe une unique fonction $\zeta(z)$ méromorphe sur $\mathbf{C}$ telle que $\zeta' = -\wp$ et $\zeta(z) = 1/z + o(z)$ en $z = 0$.

(c) Montrer qu'il existe des constantes η_1 et η_2 telles que $\zeta(z+\omega_1) = \zeta(z) + \eta_1$ et $\zeta(z+\omega_2) = \zeta(z) + \eta_2$ pour tout $z \notin \Lambda$.

(d) On suppose $\Im(\omega_2/\omega_1) > 0$. Montrer la relation de Legendre $\eta_1\omega_2 - \eta_2\omega_1 = 2\pi i$ en appliquant le théorème des résidus à ζ.

1.7. On suppose ici $\Lambda = \mathbf{Z} + \mathbf{Z}i$. Montrer que $G_6 = 0$ et en déduire l'existence de $\omega \in \frac{1}{2}\Lambda - \Lambda$ tel que $\wp(\omega) = 0$. Exprimer $\wp(iz)$ en termes de $\wp(z)$ et en déduire le diviseur de $\wp$.

1.8. Déterminer par la même méthode que l'exercice 1.7 le diviseur de $\wp$ lorsque $\Lambda = \mathbf{Z} + \mathbf{Z}j$ avec $j = e^{2i\pi/3}$.

1.9. Exprimer $\wp(2z)$ comme fraction rationnelle en $\wp(z)$ (on pourra considérer $\wp'(z)^2\wp(2z)$).

1.10. Montrer la formule d'addition pour $\wp$:

$$\wp(z_1+z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\Big(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\Big)^2 \qquad (z_2 \neq \pm z_1).$$

2. Courbes algébriques planes

Soit k un corps et $\overline{k}$ une clôture algébrique de k.

Définition 2.1. — Soit $n \geq 1$. L'*espace affine* $\mathbf{A}^n$ de dimension n sur $\overline{k}$ est $\overline{k}^n$. L'*espace projectif* $\mathbf{P}^n$ de dimension n sur $\overline{k}$ est le quotient de $\mathbf{A}^{n+1} - \{0\}$ par la relation d'équivalence $x \sim \lambda y$ pour tout $\lambda \in \overline{k}^*$.

On note $\mathbf{A}^n(k)$ l'ensemble des points de $\mathbf{A}^n$ à coordonnées dans k, et $\mathbf{P}^n(k)$ l'image de $\mathbf{A}^{n+1}(k) - \{0\}$ dans $\mathbf{P}^n$.

On note $(x_0 : \ldots : x_n)$ la classe de $(x_0, \ldots, x_n)$ dans $\mathbf{P}^n$. Un *système de coordonnées homogènes* est un représentant de $x \in \mathbf{P}^n$ dans $\mathbf{A}^{n+1} - \{0\}$.

Définition 2.2. — Un *fermé algébrique* V de $\mathbf{A}^n$ est le lieu des zéros d'une famille de polynômes $(P_i)_{i \in I}$, $P_i \in \overline{k}[X_1, \ldots, X_n]$. On note

$$V = V((P_i)_{i \in I}) = \{x = (x_1, \ldots, x_n) \in \mathbf{A}^n ; P_i(x) = 0 \text{ pour tout } i \in I\}.$$

On dit que V est *défini sur* k si l'on peut choisir les polynômes P_i à coefficients dans k. On note alors $V(k) = V \cap \mathbf{A}^n(k)$.

Remarque 2.3. — Il faut faire attention au fait que $V(k)$ ne détermine pas V en général. Par exemple si $k = \mathbf{R}$ et $V = V(X^2+1)$ alors $V(k) = \varnothing$.

Définition 2.4. — Un *fermé algébrique* V de $\mathbf{P}^n$ est le lieu des zéros d'une famille de polynômes homogènes $(P_i)_{i \in I}$, $P_i \in \overline{k}[X_0, \ldots, X_n]$. On note

$$V = V((P_i)_{i \in I}) = \{x = (x_0 : \ldots : x_n) \in \mathbf{P}^n ; P_i(x) = 0 \text{ pour tout } i \in I\}.$$

On dit que V est *défini sur* k si l'on peut choisir les polynômes P_i à coefficients dans k. On note alors $V(k) = V \cap \mathbf{P}^n(k)$.

Définition 2.5. — On dit que $C \subset \mathbf{A}^2$ est une *courbe affine plane* s'il existe un polynôme non constant $F \in \overline{k}[X, Y]$ tel que $C = V(F)$.

Définition 2.6. — On dit que $C \subset \mathbf{P}^2$ est une *courbe projective plane* s'il existe $H \in \overline{k}[X, Y, Z]$ homogène non constant tel que $C = V(H)$.

Comme $\overline{k}[X,Y]$ est factoriel, on remarque que toute courbe affine plane s'écrit $C = V(F)$ avec $F \in \overline{k}[X,Y]$ non constant et sans facteur carré, c'est-à-dire non divisible par le carré d'un polynôme irréductible.

Lemme 2.7. — *Soit H un polynôme homogène non nul de $\overline{k}[X,Y,Z]$. Si $H = H_1H_2$ alors H_1 et H_2 sont homogènes.*

Démonstration. — Soit $d = \deg H$ et $d_i = \deg H_i$. On a $d = d_1 + d_2$. Décomposons H_i en composantes homogènes, et notons H_i' la composante homogène non nulle de plus bas degré de H_i. Alors $H_1'H_2'$ est une composante homogène non nulle de H, ce qui force $H_1' = H_1$ et $H_2' = H_2$. □

Le fait que $\overline{k}[X,Y,Z]$ est factoriel et le lemme 2.7 entraînent que toute courbe projective plane s'écrit $C = V(H)$ avec $H \in \overline{k}[X,Y,Z]$ homogène non constant sans facteur carré.

Lemme 2.8. — *Soient F et G des polynômes de $\overline{k}[X,Y]$ sans facteur irréductible commun. Alors $V(F,G)$ est fini.*

Démonstration. — Les polynômes F et G sont premiers entre eux dans $\overline{k}(X)[Y]$ (sinon il existe $P \in \overline{k}[X,Y] - \overline{k}[X]$ divisant QF et QG avec $Q \in \overline{k}[X]$ non nul ; si $H \notin \overline{k}[X]$ est un facteur irréductible de P alors H divise Q, ce qui est absurde). Il existe donc une relation de Bézout $FU + GV = 1$ avec $U, V \in \overline{k}(X)[Y]$. En multipliant par un polynôme convenable en X, on obtient $V(F,G) \subset A \times \mathbf{A}^1$, où A est une partie finie de $\mathbf{A}^1$. Par symétrie, on a aussi $V(F,G) \subset \mathbf{A}^1 \times B$ avec B finie, ce qui permet de conclure. □

Lemme 2.9. — *Soient F, G deux polynômes de $\overline{k}[X,Y]$, avec F irréductible. Si $V(F) \subset V(G)$ alors F divise G.*

Démonstration. — Par hypothèse $V(F,G) = V(F)$ est infini car $\overline{k}$ est infini. Le résultat découle du lemme 2.8. □

Le lemme 2.9 entraîne que si $C = V(F)$ est une courbe affine plane avec $F \in \overline{k}[X,Y]$ sans facteur carré, le polynôme F est bien déterminé par C, à multiplication près par un élément de $\overline{k}^*$. En effet, F engendre l'idéal $I(C)$ des polynômes s'annulant sur C.

Définition 2.10. — Soit C une courbe affine plane. Une application $f : C \to \mathbf{A}^1$ est une *fonction régulière sur* C s'il existe $F \in \overline{k}[X,Y]$ tel que $f = F|_C$. On note $\overline{k}[C]$ l'anneau des fonctions régulières sur C. Si C est définie sur k, on note $k[C]$ l'image de $k[X,Y]$ dans $\overline{k}[C]$.

Le morphisme de restriction $\overline{k}[X,Y] \to \overline{k}[C]$ est surjectif et son noyau est l'idéal $I(C)$, d'où un isomorphisme $\overline{k}[C] \cong \overline{k}[X,Y]/I(C)$. On notera souvent x et y les images de X et Y dans $\overline{k}[C]$.

Théorème 2.11 **(Nullstellensatz de Hilbert)**. — *Tout idéal maximal* $\mathfrak{m}$ *de* $\overline{k}[X,Y]$ *est de la forme* $\mathfrak{m} = (X-a, Y-b)$ *avec* $a, b \in \overline{k}$.

Démonstration. — Soit $F \in \mathfrak{m}$ non nul. Alors F est non constant, et puisque $\mathfrak{m}$ est premier, on peut supposer F irréductible. Si $\mathfrak{m} = (F)$, choisissons $(a,b) \in \overline{k}^2$ tels que $F(a,b) = 0$. Alors $\mathfrak{m} \subset (X-a, Y-b)$ et la maximalité de $\mathfrak{m}$ entraîne le résultat. Sinon, soit $G \in \mathfrak{m} - (F)$. Alors F et G n'ont pas de facteur commun et la preuve du lemme 2.8 montre que $\mathfrak{m}$ contient des polynômes non nuls $R \in \overline{k}[X]$ et $S \in \overline{k}[Y]$. Comme $\overline{k}$ est algébriquement clos et $\mathfrak{m}$ est premier, on en déduit que $\mathfrak{m}$ contient $X-a$ et $Y-b$ avec $a, b \in \overline{k}$. □

Corollaire 2.12. — *Si* C *est une courbe affine plane alors tout idéal maximal de* $\overline{k}[C]$ *est de la forme* $(x-a, y-b)$ *avec* $(a,b) \in C$.

Démonstration. — Posons $C = V(F)$. Si $\mathfrak{m} \subset \overline{k}[C]$ est maximal, son image réciproque dans $\overline{k}[X,Y]$ aussi donc $\mathfrak{m} = (x-a, y-b)$ par le Nullstellensatz. On a $F \in F(a,b) + (X-a, Y-b)$ donc $(a,b) \in C$. □

Il est utile de savoir faire le lien entre les définitions affine et projective d'une courbe algébrique. On dispose d'une injection $\mathbf{A}^2 \hookrightarrow \mathbf{P}^2$ qui à (x,y) associe $(x : y : 1)$. Son image $U_{x,y}$ est une *carte affine* de $\mathbf{P}^2$. Notons que $U_{x,y} = \mathbf{P}^2 - V(Z)$ et que $V(Z) \cong \mathbf{P}^1$. On dispose également des cartes affines $U_{x,z}$ et $U_{y,z}$. Dans les propositions 2.13, 2.14 et 2.15, nous identifions $\mathbf{A}^2$ avec $U_{x,y}$ et $\mathbf{P}^1$ avec $V(Z)$.

Proposition 2.13. — *Soit* $C = V(H)$ *une courbe projective plane avec* $H \in \overline{k}[X,Y,Z]$ *homogène non constant. Si* C *rencontre* $\mathbf{A}^2$ *alors* $C \cap \mathbf{A}^2$ *est une courbe affine plane et*

$$C \cap \mathbf{A}^2 = V(F) \text{ avec } F(X,Y) = H(X,Y,1) \in \overline{k}[X,Y].$$

La courbe affine plane $C \cap \mathbf{A}^2$ est une *carte affine* de C.

Démonstration. — L'égalité $C \cap \mathbf{A}^2 = V(F)$ résulte de la définition de $U_{x,y}$. On a $F \neq 0$ et comme C rencontre $\mathbf{A}^2$, F n'est pas constant. □

Proposition 2.14. — *Soit $C = V(F)$ une courbe affine plane avec $d = \deg F \geq 1$. La plus petite courbe projective plane contenant C est*

$$\overline{C} = V(H) \text{ avec } H(X,Y,Z) = Z^d F\Big(\frac{X}{Z}, \frac{Y}{Z}\Big) \in \overline{k}[X,Y,Z].$$

Le polynôme H est l'*homogénéisé* de F. La courbe $\overline{C}$ est la *complétion projective* de C. Les points de $\overline{C} - C$ sont les *points à l'infini* de C.

Démonstration. — Le polynôme H est homogène de degré d donc $\overline{C}$ est une courbe projective plane, qui contient C car $H(X,Y,1) = F(X,Y)$. Si une courbe projective $V(H')$ contient C alors $F'(X,Y) = H'(X,Y,1)$ s'annule sur C. En décomposant F en irréductibles et en utilisant le lemme 2.9, il vient que F divise une puissance de F'. L'homogénéisé de F' divise H', donc H divise une puissance de H' et $\overline{C} \subset V(H')$. □

Proposition 2.15. — *Les applications $C \mapsto \overline{C}$ et $C \mapsto C \cap \mathbf{A}^2$ définissent une bijection entre les courbes affines planes et les courbes projectives planes ne contenant pas $\mathbf{P}^1$.*

Démonstration. — Si C est une courbe affine plane, on a $\overline{C} \cap \mathbf{A}^2 = C$ par construction et $\overline{C} \cap \mathbf{P}^1$ est fini donc $\overline{C}$ ne contient pas $\mathbf{P}^1$. Si une courbe projective plane $C = V(H)$ ne contient pas $\mathbf{P}^1$ alors H n'est pas divisible par Z donc $F(X,Y) = H(X,Y,1)$ vérifie $\deg F = \deg H$ et H est l'homogénéisé de F, d'où $\overline{C \cap \mathbf{A}^2} = C$. □

Définition 2.16. — Une courbe plane (affine ou projective) est dite *irréductible* si elle ne contient pas de courbe stricte.

Proposition 2.17. — *Soit C une courbe affine plane. Les conditions suivantes sont équivalentes :*

(1) *La courbe C est irréductible.*

(2) *La courbe $\overline{C}$ est irréductible.*

(3) *On a $C = V(F)$ avec F irréductible dans $\overline{k}[X, Y]$.*

(4) *L'anneau $\overline{k}[C]$ est intègre.*

Démonstration. — Comme la bijection de la proposition 2.15 préserve l'inclusion, on a équivalence entre (1) et (2). Montrons (1) $\Leftrightarrow$ (3). Posons $C = V(F)$ et notons F_1 un facteur irréductible de F. Alors $V(F_1) \subset V(F)$ et par irréductibilité de C, il vient $C = V(F_1)$. Réciproquement, supposons $C = V(F)$ avec F irréductible. Si C contient $C' = V(G)$ avec G non constant et sans facteur carré, alors G divise F (lemme 2.9) d'où G irréductible et $C' = C$. Enfin, montrons (3) $\Leftrightarrow$ (4). Posons $C = V(F)$ avec F non constant et sans facteur carré. Alors $\overline{k}[C] \cong \overline{k}[X, Y]/(F)$ est intègre si et seulement si F est irréductible ($\overline{k}[X, Y]$ est factoriel). □

Définition 2.18. — Soit C une courbe affine plane irréductible. On appelle corps des *fonctions rationnelles sur C* et on note $\overline{k}(C)$ le corps des fractions de l'anneau intègre $\overline{k}[C]$. Si de plus C est définie sur k, on note $k(C)$ le corps des fractions de $k[C]$.

Définition 2.19. — Soit C une courbe affine plane irréductible. Si $f \in \overline{k}(C)$ est une fonction rationnelle et $P \in C$, on dit que f est *régulière en P* s'il existe $g, h \in \overline{k}[C]$ avec $h(P) \neq 0$ telles que $f = g/h$; on pose alors $f(P) = g(P)/h(P)$.

Remarque 2.20. — Il se peut que $f = g/h$ avec $h(P) = 0$ mais que f soit quand même régulière en P. Par exemple $C = V(X^2 + Y^2 - 1)$ est irréductible et la fonction rationnelle $f = (x - 1)/y$ est régulière en $(1, 0)$. En effet $f = -y/(x + 1)$ donc $f(1, 0) = 0$ si $\mathrm{car}(k) \neq 2$; on a $C = V(X + Y + 1)$ et $f = 1$ si $\mathrm{car}(k) = 2$.

Exemple 2.21. — Si $C = \mathbf{A}^1 = V(Y)$ alors $k[C] = k[X]$ et $k(C) = k(X)$: une fonction régulière sur $\mathbf{A}^1$ est simplement un polynôme, tandis qu'une fonction rationnelle sur $\mathbf{A}^1$ est une fraction rationnelle.

Lemme 2.22. — *Soit C une courbe affine plane irréductible.*

(1) *Si $f \in \overline{k}(C)$, il existe $S \subset C$ fini tel que f est régulière sur $C - S$.*

(2) *Si $f_1, f_2 \in \overline{k}(C)$ coïncident hors d'un ensemble fini alors $f_1 = f_2$.*

Démonstration. — Si $f = g/h$ avec $h \neq 0$ alors l'ensemble S des zéros de h dans C est fini d'après le lemme 2.9, et f est définie sur $C - S$.

Supposons $f_1 = g_1/h_1$ et $f_2 = g_2/h_2$ définies et égales sur $C - S$ avec S fini. Alors la fonction régulière $g_1h_2 - g_2h_1$ est nulle sur l'ensemble infini $C - S$, ce qui entraîne $g_1h_2 = g_2h_1$ et $f_1 = f_2$. □

La proposition suivante justifie la terminologie de fonction régulière.

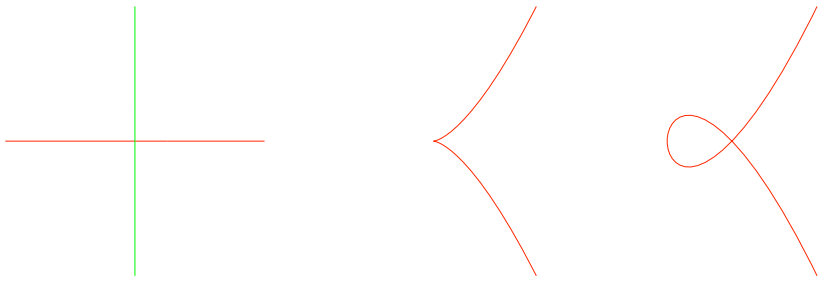
Proposition 2.23. — *Soit C une courbe affine plane irréductible. Si $f \in \overline{k}(C)$ est régulière sur C alors $f \in \overline{k}[C]$.*

Démonstration. — Considérons l'idéal $I = \{h \in \overline{k}[C]; hf \in \overline{k}[C]\}$ et supposons par l'absurde $I \neq \overline{k}[C]$. Alors I est inclus dans un idéal maximal $(x-a, y-b)$ avec $(a, b) \in C$. Comme f est régulière en (a, b), il vient $f = g/h$ avec $h(a, b) \neq 0$. On a alors $h \in I$, une contradiction. □

Soit C une courbe affine plane irréductible. Si U est une carte affine de $\mathbf{P}^2$ rencontrant C, on peut voir $\overline{C}$ comme la complétion projective de la courbe affine $C' = \overline{C} \cap U$ (proposition 2.15). Montrons que les corps des fonctions rationnelles sur C et C' coïncident. Supposons par exemple $U = U_{x,z}$. Cherchons les coordonnées de $Q = (x, y) \in C \cap U$ dans la carte affine C'. On a $y \neq 0$ donc $Q = (x : y : 1) = (x/y : 1 : 1/y)$ et les coordonnées de Q dans C' sont $(x', z') = (x/y, 1/y)$. On définit un morphisme de changement de carte $\phi : \overline{k}[X', Z'] \to \overline{k}(C)$ par $\phi(X') = x/y$ et $\phi(Z') = 1/y$. Notons que ϕ est bien défini car $y \in \overline{k}[C] - \{0\}$ (sinon $\overline{C} \subset V(Y)$).

Lemme 2.24. — *Le morphisme ϕ induit $\overline{k}(C') \cong \overline{k}(C)$.*

Démonstration. — Posons $C = V(F)$, $\overline{C} = V(H)$, et $d = \deg H$. On a $C' = V(G)$ avec $G(X', Z') = H(X', 1, Z')$ d'où $\phi(G) = H(x/y, 1, 1/y) = y^{-d}H(x, y, 1) = y^{-d}F(x, y) = 0$. Donc ϕ induit $\overline{k}[C'] \to \overline{k}(C)$. Si $f \in \overline{k}[C']$ est non nulle alors il existe $Q \in C \cap U$ tel que $f(Q) \neq 0$ (lemme 2.22(2)), donc $\phi(f)$ est non nulle en Q et $\phi(f) \neq 0$. On peut ainsi passer au corps des fractions et obtenir un morphisme injectif $\phi : \overline{k}(C') \to \overline{k}(C)$. Par symétrie, on a également $\psi : \overline{k}(C) \to \overline{k}(C')$ avec $\phi \circ \psi = \mathrm{id}$, donc ϕ est un isomorphisme. □



(a) $xy = 0$ (b) $y^2 = x^3$ (c) $y^2 = x^3 + x^2$

FIG. 3. Courbes planes singulières

Soit C une courbe projective plane irréductible. Le corps $\overline{k}(C)$ des *fonctions rationnelles sur* C est le corps des fonctions rationnelles sur une carte affine de C. D'après le lemme 2.24, cette définition ne dépend pas de la carte affine choisie. Une fonction $f \in \overline{k}(C)$ est *régulière* en $P \in C$ si elle l'est dans une carte affine contenant P.

Définition 2.25. — Soit $C = V(F)$ une courbe affine plane avec $F \in \overline{k}[X, Y]$ sans facteur carré. On dit que C est *lisse* ou *non singulière* en $P = (x_0, y_0) \in C$ si $(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y})(P) \neq (0, 0)$. Dans ce cas, la *tangente* de C en P est donnée par

$$T_P C : \frac{\partial F}{\partial X}(P) \cdot (X - x_0) + \frac{\partial F}{\partial Y}(P) \cdot (Y - y_0) = 0.$$

On dit que C est lisse lorsqu'elle est lisse en tous ses points.

Exemples 2.26. — (1) La courbe $C = \mathbf{A}^1 = V(Y) \subset \mathbf{A}^2$ est lisse.

(2) La courbe $C = V(X^2 + Y^2 - 1) \subset \mathbf{A}^2$ est lisse : c'est vrai si $\mathrm{car}(k) \neq 2$ et on a $C = V(X + Y + 1)$ lorsque $\mathrm{car}(k) = 2$.

(3) Les courbes affines planes $V(XY)$, $V(Y^2 - X^3)$ et $V(Y^2 - X^3 - X^2)$ ne sont pas lisses en $(0, 0)$, cf. figure 3. La première n'est pas irréductible, les deux autres le sont (exercice 2.4).

Une courbe projective plane C est lisse en $P \in C$ si elle l'est dans une carte affine contenant P. Cette définition est indépendante de la carte affine (exercice 2.3).

Définition 2.27. — Soit C une courbe affine plane et $P \in C$. On note $\mathfrak{m}_P$ l'idéal de $\overline{k}[C]$ formé des fonctions s'annulant en P.

L'évaluation en P fournit un isomorphisme $\overline{k}[C]/\mathfrak{m}_P \cong \overline{k}$, donc $\mathfrak{m}_P$ est maximal. De plus $\mathfrak{m}_P/\mathfrak{m}_P^2$ est un $\overline{k}[C]/\mathfrak{m}_P$-module, c'est-à-dire un $\overline{k}$-espace vectoriel.

Proposition 2.28. — *Soit C une courbe affine plane et $P \in C$. Alors* $\dim_{\overline{k}} \mathfrak{m}_P/\mathfrak{m}_P^2 \geq 1$ *avec égalité si et seulement si P est lisse.*

Démonstration. — Quitte à effectuer une translation des données, on peut supposer $P = (0,0)$. L'image réciproque I de $\mathfrak{m}_P$ dans $\overline{k}[X,Y]$ est formé des polynômes s'annulant en $(0,0)$ donc $I = (X,Y)$ et $\mathfrak{m}_P = (x,y)$. On en déduit que le $\overline{k}$-espace vectoriel $\mathfrak{m}_P/\mathfrak{m}_P^2$ est engendré par les classes $\overline{x}$ et $\overline{y}$. Posons $C = V(F)$ avec $F \in \overline{k}[X,Y]$ sans facteur carré. Si C n'est pas lisse en P, on a $F \in I^2 = (X^2, XY, Y^2)$ donc $a\overline{x} + b\overline{y} = 0$ avec $a, b \in \overline{k}$ entraîne $aX + bY \in I^2$ et donc $a = b = 0$. Ainsi $\dim_{\overline{k}} \mathfrak{m}_P/\mathfrak{m}_P^2 = 2$. Si C est lisse en P, le développement de Taylor à l'ordre 1 de F en P montre que $F \equiv \frac{\partial F}{\partial X}(P) \cdot X + \frac{\partial F}{\partial Y}(P) \cdot Y \pmod{I^2}$ ce qui implique $\frac{\partial F}{\partial X}(P) \cdot \overline{x} + \frac{\partial F}{\partial Y}(P) \cdot \overline{y} = 0$ dans $\mathfrak{m}_P/\mathfrak{m}_P^2$. De plus $\overline{x} = \overline{y} = 0$ entraînerait $X, Y \in I^2 + (F)$ et donc $I = I^2 + (F)$ et le $\overline{k}$-espace vectoriel I/I^2 de base $(\overline{X}, \overline{Y})$ serait engendré par la classe de F, ce qui est absurde. □

Toute fonction régulière $f \in \overline{k}[C]$ s'écrit $f = f(P) + h$ avec $h \in \mathfrak{m}_P$. La *différentielle* de f en P est la classe de h dans $\mathfrak{m}_P/\mathfrak{m}_P^2$; on la note $df(P)$. On vérifie les règles usuelles du calcul différentiel : on a $d(f+g)(P) = df(P) + dg(P)$ et $d(fg)(P) = f(P)dg(P) + g(P)df(P)$.

Définition 2.29. — Soit C une courbe projective plane irréductible et $P \in C$. L'*anneau local* de C en P est $\mathcal{O}_{C,P} = \{f \in \overline{k}(C) ; f \text{ régulière en } P\}$. On note $\mathfrak{m}_{C,P}$ l'idéal $\{f \in \mathcal{O}_{C,P} ; f(P) = 0\}$.

L'évaluation en P fournit $\mathcal{O}_{C,P}/\mathfrak{m}_{C,P} \cong \overline{k}$ comme dans le cas affine.

Lemme 2.30. — *Soit C une courbe projective plane irréductible et P un point lisse de C. Alors l'idéal $\mathfrak{m}_{C,P}$ est principal.*

Démonstration. — Soit C_0 une carte affine de C contenant P, et $\mathfrak{m}_P$ l'idéal maximal de $\overline{k}[C_0]$ associé à P. Nous allons montrer plus précisément

que tout $t \in \mathfrak{m}_P - \mathfrak{m}_P^2$ engendre $\mathfrak{m}_{C,P}$. L'idéal $\mathfrak{m}_{C,P}$ est engendré par $\mathfrak{m}_{C,P} \cap \overline{k}[C_0] = \mathfrak{m}_P$: si $f = g/h \in \mathfrak{m}_{C,P}$ alors $g \in \mathfrak{m}_P$ et $1/h \in \mathcal{O}_{C,P}^*$. Comme $\overline{k}[C_0]$ est noethérien, le module $\mathfrak{m}_{C,P}/(t)$ est de type fini sur $\mathcal{O}_{C,P}$. Posons $\mathfrak{m}_{C,P} = (t, t_1, \ldots, t_r)$ avec r minimal, et supposons par l'absurde $r \geq 1$. D'après la proposition 2.28, on a $\mathfrak{m}_{C,P} = (t, \mathfrak{m}_{C,P}^2)$ d'où $t_r = f_1 t_1 + \cdots + f_r t_r + ft$ avec $f_i \in \mathfrak{m}_{C,P}$ et $f \in \mathcal{O}_{C,P}$. Or $1 - f_r \in \mathcal{O}_{C,P}^*$ donc $t_r \in (t, t_1, \ldots, t_{r-1})$, contredisant la minimalité de r. □

Définition 2.31. — Soit C une courbe projective plane irréductible lisse en $P \in C$. Une *uniformisante* en P est un générateur de $\mathfrak{m}_{C,P}$.

Proposition 2.32. — *Soit C une courbe projective plane irréductible et t une uniformisante en un point lisse P de C. Tout $f \in \overline{k}(C)^*$ s'écrit de manière unique $f = t^n u$ avec $n \in \mathbf{Z}$ et $u \in \mathcal{O}_{C,P}^*$.*

Démonstration. — Si $t^m u = t^n v$ avec $m < n$ alors $t^{n-m} = u/v$ et on a une contradiction en évaluant en P, d'où l'unicité. Pour l'existence, supposons dans un premier temps que f est régulière en P. Si $f \in (t^n)$ pour tout $n \geq 1$ alors $f = t^n f_n$ avec $f_n = t f_{n+1}$. La suite d'idéaux (f_n) étant croissante et $\mathcal{O}_{C,P}$ étant noethérien (tout idéal I de $\mathcal{O}_{C,P}$ est engendré par $I \cap \overline{k}[C_0]$, où C_0 est une carte affine de C), il existe N tel que $(f_N) = (f_{N+1})$. Alors $f_{N+1} = f_N g$ avec $g \in \mathcal{O}_{C,P}$, d'où $gt = 1$, une contradiction en évaluant en P. Il existe donc un entier $n \geq 0$ maximal tel que $f \in (t^n)$. On a alors $f = t^n u$, mais $u(P) \neq 0$ par maximalité de n, d'où l'existence. Si f est quelconque, on peut l'écrire comme quotient de deux fonctions régulières en P, ce qui nous ramène au premier cas. □

Dans la proposition 2.32, l'entier n ne dépend que de f : si t' est une autre uniformisante en P alors $t = ht'$ avec $h \in \mathcal{O}_{C,P}^*$ donc $f = t'^n h^n u$ avec $h^n u \in \mathcal{O}_{C,P}^*$. L'entier n est appelé *ordre de f en P* et est noté $\mathrm{ord}_P(f)$. Si C est lisse, le *diviseur de f* est la somme formelle

$$(f) = \mathrm{div}\, f = \sum_{P \in C} \mathrm{ord}_P(f) \cdot [P] \in \mathbf{Z}[C].$$

Un tel diviseur est dit *principal*. Notons que cette somme est finie (appliquer le lemme 2.22(1) à f et $1/f$).

Lemme 2.33. — *Soit C une courbe projective plane irréductible. Si $f \in \overline{k}(C)$ est non constante, alors $\overline{k}(f) \subset \overline{k}(C)$ est une extension finie.*

Démonstration. — Posons $C = \overline{C_0}$. Comme C_0 n'est pas réduite à un point, l'une des fonctions régulières x ou y est non constante, disons x. Alors x est transcendant sur $\overline{k}$ et par construction de $\overline{k}(C)$, l'extension $\overline{k}(x) \subset \overline{k}(C)$ est finie, engendrée par y. En multipliant le polynôme minimal de f sur $\overline{k}(x)$ par un polynôme convenable de $\overline{k}[x]$, on obtient une relation algébrique $Q(x, f) = 0$ avec $Q \in \overline{k}[X, T]$ non nul. Comme $f \notin \overline{k}$, on ne peut avoir $Q \in \overline{k}[T]$, ce qui montre que x est algébrique sur $\overline{k}(f)$. Enfin y est algébrique sur $\overline{k}(x, f)$ donc sur $\overline{k}(f)$. □

Définition 2.34. — Le *degré* d'une fonction rationnelle $f \in \overline{k}(C)$ non constante est le degré de l'extension $\overline{k}(f) \subset \overline{k}(C)$.

Théorème 2.35. — *Soit C une courbe projective plane irréductible et lisse. Pour tout $f \in \overline{k}(C)$ non constante, on a*

$$\deg(f) = \sum_{\substack{P \in C \\ \mathrm{ord}_P(f) \geq 0}} \mathrm{ord}_P(f).$$

Démonstration. — Notons $n = \deg(f)$. Notons B la fermeture intégrale de $A = \overline{k}[f]$ dans $\overline{k}(C)$. Montrons que B est un anneau de Dedekind. Par définition, B est intègre et intégralement clos. Montrons que B est noethérien. Soit I un idéal non nul de B. Si $g \in I$ est non nul, g vérifie une équation $g^d + a_{d-1}g^{d-1} + \cdots + a_1 g + a_0 = 0$ avec $a_i \in A$ et on peut supposer $a_0 \neq 0$. Alors $a_0 \in I$ et pour montrer que I est de type fini, il suffit de montrer que $I/(a_0)$ est de dimension finie sur $\overline{k}$. Si J est un sous-A-module de type fini de I, il est libre car A est principal, et son rang est $\leq n$ puisque toute famille libre sur A est libre sur $\overline{k}(f)$. De plus J/a_0J est un $\overline{k}$-espace vectoriel de dimension $\leq mn$ avec $m = \dim_{\overline{k}} A/(a_0)$. Supposons par l'absurde que $I/(a_0)$ possède une famille $\overline{k}$-libre $(\overline{x_1}, \ldots, \overline{x_{mn+1}})$. Posant $J = \sum Ax_i$, la famille $(\overline{x_i})$ est liée dans J/a_0J et donc dans $I/(a_0)$, ce qui est absurde. Ainsi I est de type fini sur B. Enfin, montrons que tout idéal premier $\mathfrak{p}$ non nul de B est maximal. On a vu que l'anneau intègre $B/\mathfrak{p}$ est un $\overline{k}$-espace vectoriel de dimension

finie (prendre $I = B$ ci-dessus), c'est donc un corps et on a même $B/\mathfrak{p} \cong \overline{k}$ car $\overline{k}$ est algébriquement clos.

Considérons l'idéal premier (f) de A. Par la théorie générale des anneaux de Dedekind (cf. cours de théorie algébrique des nombres), on a $fB = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_\mathfrak{r}^{e_r}$ avec $\mathfrak{p}_i$ idéal maximal de B. Par la même démonstration que celle utilisée pour les anneaux d'entiers de corps de nombres, on a l'égalité $n = \sum_{i=1}^{r} e_i$ car $f_i = \dim_{\overline{k}} B/\mathfrak{p}_i = 1$. Nous allons faire le lien entre les $\mathfrak{p}_i$ et les points où f s'annule ; l'exposant e_i sera égal à l'ordre d'annulation correspondant.

Si f est régulière et s'annule en $P \in C$, montrons que $B \subset \mathcal{O}_{C,P}$. Soit $t \in \overline{k}(C)$ une uniformisante en P. Tout $g \in B$ vérifie une équation $g^d + a_{d-1}g^{d-1} + \cdots + a_1 g + a_0 = 0$ avec $a_i \in A$, et si $\mathrm{ord}_P(g) = m < 0$ on a $\mathrm{ord}_P(a_i g^i) \geq \mathrm{ord}_P(g^i) > dm$ d'où une contradiction en multipliant l'équation précédente par t^{-dm} et en évaluant en P. Alors $\mathfrak{p} = \mathfrak{m}_{C,P} \cap B$ est un idéal premier qui contient f donc il existe i tel que $\mathfrak{p} = \mathfrak{p}_i$. De plus, si $h \in B - \mathfrak{p}_i$ alors h est inversible dans $\mathcal{O}_{C,P}$ donc $\mathcal{O}_{C,P}$ contient $B_i = \{g/h; g, h \in B, h \notin \mathfrak{p}_i\}$. Montrons que B_i est un sous-anneau maximal de $\overline{k}(C)$, ce qui entraînera $B_i = \mathcal{O}_{C,P}$. Soit $z \notin B_i$. On a $zB = \mathfrak{p}_i^{n_i} I/J$ avec des idéaux I, J de B premiers à $\mathfrak{p}_i$. Si $n_i \geq 0$ alors $zJ \subset B$ et en utilisant $J \not\subset \mathfrak{p}_i$, on a $z \in B_i$, ce qui est absurde. Donc $n_i < 0$. Si $g \in \overline{k}(C)$, alors pour m assez grand l'exposant de $\mathfrak{p}_i$ dans la décomposition en idéaux premiers de g/z^m est ≥ 0, d'où $g/z^m \in B_i$, ce qui entraîne $\overline{k}(C) = B_i[z]$, et la maximalité de B_i. L'idéal engendré par $\mathfrak{p}_i$ dans B_i est $\mathfrak{p}_i B_i = \{g/h; g \in \mathfrak{p}_i, h \notin \mathfrak{p}_i\}$. Il en résulte que tout élément de $B_i - \mathfrak{p}_i B_i$ est inversible dans B_i et que $\mathfrak{p}_i B_i$ est maximal dans B_i, d'où $\mathfrak{p}_i B_i = \mathfrak{m}_{C,P}$. Alors $fB_i = \mathfrak{m}_{C,P}^{e_i}$ ce qui signifie $e_i = \mathrm{ord}_P(f)$.

L'application $P \mapsto \mathfrak{p}_i$ ci-dessus est injective car si $\mathfrak{m}_{C,P} = \mathfrak{m}_{C,P'}$, où P et P' appartiennent à la même carte affine C_0 (on peut s'y ramener par un changement projectif de coordonnées), alors $\mathfrak{m}_P = \mathfrak{m}_{P'}$ donc $P = P'$. Il reste à montrer la surjectivité.

Soit $1 \leq i \leq r$. Grâce à $B/\mathfrak{p}_i \cong \overline{k}$ on montre que $B_i = B + \mathfrak{p}_i B_i$ d'où un isomorphisme $B/\mathfrak{p}_i \cong B_i/\mathfrak{p}_i B_i$. Notons $C = \overline{C_0}$, où C_0 est munie des coordonnées usuelles x et y. Supposons dans un premier temps que $x, y \in B_i$. Alors $\overline{k}[C_0] \subset B_i$ et $\mathfrak{m} = \mathfrak{p}_i B_i \cap \overline{k}[C_0]$ est un idéal maximal de $\overline{k}[C_0]$: on a une injection $\overline{k}[C_0]/\mathfrak{m} \to B_i/\mathfrak{p}_i B_i \cong \overline{k}$ et la composition

$\overline{k} \to \overline{k}[C_0]/\mathfrak{m} \to \overline{k}$ est l'identité. Par le Nullstellensatz, il existe $P \in C_0$ tel que $\mathfrak{m} = \mathfrak{m}_P$. Tout $h \in \overline{k}[C_0] - \mathfrak{m}_P$ est inversible dans B_i d'où une inclusion $\mathcal{O}_{C,P} \subset B_i$, qui est une égalité car $\mathcal{O}_{C,P}$ est un sous-anneau maximal de $\overline{k}(C)$. Il en résulte $f \in \mathfrak{p}_i B_i = \mathfrak{m}_{C,P}$ et $\mathfrak{p}_i$ est associé à P.

Si $y \neq 0$ et $x/y \in B_i$ alors $1/y \in B_i$ (sinon $x, y \in B_i$) et l'on peut refaire le raisonnement ci-dessus dans la carte affine $C_1 = C \cap U_{x,z}$: il existe $P \in C_1$ tel que $\mathfrak{p}_i$ est associé à P. Sinon on a $x \neq 0$ et $y/x, 1/x \in B_i$ donc on peut utiliser la carte $C_2 = C \cap U_{y,z}$. □

Corollaire 2.36. — *Soit C une courbe projective plane irréductible et lisse. Alors tout diviseur principal est de degré* 0.

Démonstration. — Le degré de div f vaut $\deg(f) - \deg(1/f) = 0$. □

Corollaire 2.37. — *Soit C une courbe projective plane irréductible. Si $f \in \overline{k}(C)$ est régulière sur C alors f est constante.*

Démonstration. — Si f n'est pas constante alors $1/f$ ne s'annule pas sur C donc $\deg(1/f) = 0$, ce qui est absurde. □

Remarque 2.38. — Le nombre de préimages de $a \in \overline{k}$ par f (comptées avec multiplicité) ne dépend pas de a : il vaut $\deg(f - a) = \deg(f)$.

Définition 2.39. — Soit C une courbe projective plane irréductible. L'espace $\Omega^1(\overline{k}(C))$ des *formes différentielles rationnelles* sur C est le $\overline{k}(C)$-espace vectoriel engendré par les symboles df, avec $f \in \overline{k}(C)$, et quotienté par les relations suivantes

$$d(f+g) = df + dg \qquad d(\lambda f) = \lambda df \qquad (f, g \in \overline{k}(C); \lambda \in \overline{k})$$
$$d(fg) = f dg + g df \qquad (f, g \in \overline{k}(C)).$$

Si C est définie sur k, on note $\Omega^1(k(C))$ le sous-$k(C)$-espace vectoriel de $\Omega^1(\overline{k}(C))$ engendré par les df avec $f \in k(C)$.

Proposition 2.40. — *Soit C une courbe projective plane irréductible. L'espace vectoriel $\Omega^1(\overline{k}(C))$ est de dimension* 1 *sur $\overline{k}(C)$. Si t est une uniformisante en un point lisse de C, alors dt est une base de $\Omega^1(\overline{k}(C))$.*

Démonstration. — Comme C possède des points lisses (poser $C = \overline{C_0}$, $C_0 = V(F)$ et utiliser le lemme 2.9 avec $G = \partial F/\partial X$ ou $\partial F/\partial Y$), il existe des uniformisantes, et il suffit de montrer la seconde assertion.

Soit t une uniformisante en $P \in C$. D'après le lemme 2.33, l'extension $\overline{k}(t) \subset \overline{k}(C)$ est finie. Montrons qu'elle est séparable. Il suffit de traiter le cas $\mathrm{car}(k) = p > 0$. Soit $f \in \overline{k}(C)$. Prenons $Q \in \overline{k}[X,T]$ de degré minimal ≥ 1 en X tel que $Q(f,t) = 0$ (il en existe puisque l'extension est finie). Si $\partial Q/\partial X$ est non nul alors f est séparable sur $\overline{k}(t)$. On peut donc supposer $Q(X,T) = R(X^p,T)$ avec $R \in \overline{k}[X,T]$. Posons $R = \sum_{j=0}^{p-1} R_j(X,T^p)T^j$ avec $R_j \in \overline{k}[X,T]$. Si l'on note S_j le polynôme dont les coefficients sont les racines p-ièmes des coefficients de R_j, alors $Q(X,T) = \sum_{j=0}^{p-1} R_j(X^p,T^p)T^j = \sum_{j=0}^{p-1} S_j(X,T)^p T^j$. Si $S_j(f,t) \neq 0$ alors l'ordre de $S_j(f,t)t^j$ au point P est $\equiv j \pmod p$. En considérant l'ordre en P, la relation $Q(f,t) = 0$ force $S_j(f,t) = 0$ pour tout j. Mais l'un des polynômes S_j dépend effectivement de X, ce qui contredit la minimalité du degré de Q puisque $p \deg_X S_j \leq \deg_X Q$.

Si A est un anneau et B une A-algèbre, une dérivation de A dans B est un morphisme de groupes $D : A \to B$ vérifiant $D(ab) = aD(b) + bD(a)$ pour tout $a, b \in A$. Soit $D : \overline{k}(t) \to \overline{k}(t)$ la dérivation par rapport à t. Alors D se prolonge en une unique dérivation $\overline{k}$-linéaire $\widetilde{D} : \overline{k}(C) \to \overline{k}(C)$. En effet, l'extension $\overline{k}(t) \subset \overline{k}(C)$ est finie séparable donc monogène : posons $\overline{k}(C) = \overline{k}(t)[f]$ et notons $\mu = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \overline{k}(t)[X]$ le polynôme minimal de f. On doit avoir $\mu'(f)\widetilde{D}(f) + \sum_{i=0}^{n-1} D(a_i)f^i = 0$ ce qui détermine de manière unique $\widetilde{D}(f)$ donc $\widetilde{D}$. En posant $\widehat{D}(X) = -\mu'(f)^{-1} \sum_{i=0}^{n-1} D(a_i)f^i$, on définit une dérivation $\overline{k}$-linéaire $\widehat{D} : \overline{k}(t)[X] \to \overline{k}(C)$ (la structure d'algèbre étant donnée par $X \mapsto f$) qui annule l'idéal engendré par μ, d'où l'existence de $\widetilde{D}$.

Comme $\widetilde{D}$ est une dérivation, le passage au quotient fournit une forme linéaire $\lambda : \Omega^1(\overline{k}(C)) \to \overline{k}(C)$ telle que $\lambda(dg) = \widetilde{D}(g)$ pour tout $g \in \overline{k}(C)$. Comme $\lambda(dt) = D(t) = 1$, on a $dt \neq 0$ et donc $\Omega^1(\overline{k}(C)) \neq \{0\}$. De plus, en appliquant d à $\mu(f) = 0$, on trouve $\mu'(f)df \in \overline{k}(C) \cdot dt$ par le même calcul qu'avant, d'où $df \in \overline{k}(C) \cdot dt$ et par suite $\Omega^1(\overline{k}(C)) = \overline{k}(C) \cdot dt$. □

Définition 2.41. — Soit C une courbe projective plane irréductible. On dit que $\omega \in \Omega^1(\overline{k}(C))$ est *régulière* en $P \in \overline{C}$ si on peut écrire $\omega = \sum_{i=1}^n f_i dg_i$ avec toutes les f_i et g_i régulières en P.

Lemme 2.42. — *Supposons C lisse en P, et soit t une uniformisante en P. Alors ω est régulière en P si et seulement si $\omega = f dt$ avec f régulière en P.*

Démonstration. — La condition est visiblement suffisante. Pour montrer le sens direct, introduisons le développement d'une fonction rationnelle en série de Laurent.

Toute fonction $f \in \mathcal{O}_{C,P}$ peut s'écrire $f = a_0 + tf_1$ avec $a_0 = f(P) \in \overline{k}$ et $f_1 \in \mathcal{O}_{C,P}$. En itérant ce procédé, on voit qu'il existe une unique série formelle $i(f) = \sum_{n \geq 0} a_n T^n \in \overline{k}[[T]]$ telle que $f \in \sum_{n=0}^N a_n t^n + (t^{N+1})$ pour tout $N \geq 0$. L'application $i : \mathcal{O}_{C,P} \to \overline{k}[[T]]$ est un morphisme d'anneaux injectif (d'après la démonstration de la proposition 2.32, on a $\cap(t^n) = \{0\}$). En passant aux corps des fractions, on obtient un morphisme injectif i de $\overline{k}(C)$ dans le corps $\overline{k}((T))$ des séries de Laurent à coefficients dans $\overline{k}$. De plus $\mathcal{O}_{C,P}$ est la préimage de $\overline{k}[[T]]$ par i.

Dans la preuve de la proposition 2.40, on a construit une dérivation $\overline{k}$-linéaire $\widetilde{D} : \overline{k}(C) \to \overline{k}(C)$ telle que $\widetilde{D}(t) = 1$. Le corps $\overline{k}((T))$ est lui aussi muni d'une dérivation D_T, à savoir la dérivation (formelle) par rapport à T. On a en fait $D_T \circ i = i \circ \widetilde{D}$. En effet, les deux membres sont des dérivations $\overline{k}$-linéaires de $\overline{k}(C)$ dans $\overline{k}((T))$ (que l'on considère comme $\overline{k}(C)$-espace vectoriel via i) qui coïncident en t, donc sur $\overline{k}(t)$ puis sur $\overline{k}(C)$ par le même argument que précédemment.

Pour montrer la proposition, il suffit de considérer le cas $\omega = dg$ avec g régulière en P. On a $dg = f dt$ avec $f \in \overline{k}(C)$. Par construction de $\widetilde{D}$, on a $f = \widetilde{D}(g)$ donc $i(f) = D_T(i(g)) \in \overline{k}[[T]]$. □

Définition 2.43. — Soit C une courbe projective plane irréductible. On note $\Omega^1(C)$ l'espace des formes différentielles rationnelles sur C qui sont régulières en tout point de C. Le *genre* de C est $\dim_{\overline{k}} \Omega^1(C)$.

Théorème 2.44. — *Toute courbe projective plane lisse est irréductible et son genre est donné par $(d-1)(d-2)/2$, où d est le degré d'un polynôme irréductible qui la définit.*

Démonstration. — Soit $C = V(H)$ une courbe projective plane lisse avec H sans facteur carré. Montrons que H est irréductible. Supposons $H = H_1H_2$ avec H_1 irréductible et $d_2 = \deg H_2 \geq 1$. Comme les dérivées premières de H s'annulent sur $V(H_1, H_2)$, ce dernier ensemble est vide (exercice 2.3). Quitte à faire un changement projectif de coordonnées, on peut supposer $D = V(Z)$ non contenue dans $C_1 = V(H_1)$. La fonction rationnelle $f = 1/H_2(x, y) \in \overline{k}(C_1)^*$ est régulière sur C_1, donc constante par le corollaire 2.37, mais alors $V(H_1, H_2)$ contient l'ensemble non vide $C_1 \cap D$, ce qui est absurde. Ainsi C est irréductible.

La courbe C est la complétion projective de $C_0 = V(F)$ avec $F \in \overline{k}[X, Y]$ irréductible de degré $d \geq 1$. Montrons que quitte à faire un changement de variables affine, on peut supposer F unitaire de degré d en X. Notons $\sum_{j=0}^{d} a_j X^j Y^{d-j}$ la composante homogène de degré d de F. En posant $X = X'$ et $Y = Y' + \lambda X'$, $\lambda \in \overline{k}$, le coefficient de X'^d dans F vaut $\sum_{j=0}^{d} a_j \lambda^{d-j}$, ce qui peut être rendu non nul pour λ bien choisi car les a_j ne sont pas tous nuls.

Soit $F_X = \partial F/\partial X$ et $F_Y = \partial F/\partial Y$. En différentiant la relation $F(x, y) = 0$, il vient $F_X(x, y)dx + F_Y(x, y)dy = 0$. Posons

$$\omega_R = R(x, y)\frac{dx}{F_Y(x, y)} = -R(x, y)\frac{dy}{F_X(x, y)} \qquad (R \in \overline{k}[X, Y]).$$

Comme C_0 est lisse, on a $(F_X, F_Y) \neq (0, 0)$ donc ω_R est régulière sur C_0. Nous allons montrer que l'application $R \mapsto \omega_R$ induit un isomorphisme entre l'espace vectoriel des polynômes de $\overline{k}[X, Y]$ de degré $\leq d - 3$ et $\Omega^1(C)$, d'où la formule pour le genre de C.

Soit $R \in \overline{k}[X, Y]$ et $P = (x_P : y_P : 0) \in C - C_0$. Comme $H(x_P, 0, 0) = x_P^d$, on a nécessairement $y_P \neq 0$. On considère donc la carte affine $C_1 = C \cap U_{x,z}$. On a $C_1 = V(G)$ avec $G(X, Z) = H(X, 1, Z)$. Le changement de carte est $x' = x/y$ et $z' = 1/y$, ce qui donne

$$\omega_R = -R(x'/z', 1/z')\frac{d(1/z')}{F_X(x'/z', 1/z')} = \frac{R(x'/z', 1/z')dz'}{z'^2 F_X(x'/z', 1/z')}.$$

Le polynôme $H_X = \partial H/\partial X$ est homogène de degré $d - 1$; on a donc $F_X(\frac{x'}{z'}, \frac{1}{z'}) = H_X(\frac{x'}{z'}, \frac{1}{z'}, 1) = H_X(x', 1, z')/z'^{d-1} = G_X(x', z')/z'^{d-1}$ avec $G_X = \partial G/\partial X$. Il vient ainsi

$$\omega_R = z'^{d-3} R\Big(\frac{x'}{z'}, \frac{1}{z'}\Big) \frac{dz'}{G_X(x', z')} = -z'^{d-3} R\Big(\frac{x'}{z'}, \frac{1}{z'}\Big) \frac{dx'}{G_Z(x', z')}$$

avec $G_Z = \partial G / \partial Z$. Si $\deg R \leq d-3$ alors $z'^{d-3} R(x'/z', 1/z') \in \overline{k}[C_1]$ d'où ω_R régulière sur C_1 et donc sur C.

Soit maintenant $\omega \in \Omega^1(C)$. Comme ω est régulière sur C_0, on a $\omega = \omega_R$ avec $R \in \overline{k}[X, Y]$ (proposition 2.23 et lemme 2.42). En utilisant de la même façon l'expression de ω_R en termes de x' et z', la fonction rationnelle $f = z'^{d-3} R\big(\frac{x'}{z'}, \frac{1}{z'}\big)$ est régulière sur C_1. Comme F est unitaire de degré d en X, on peut remplacer R par son reste dans la division euclidienne par F et supposer $\deg_X R \leq d-1$. Supposons par l'absurde $r = \deg R > d-3$. Comme G est unitaire de degré d en X, on a $\overline{k}[C_1] \cong \overline{k}[X, Z]/(G) \cong \oplus_{i=0}^{d-1} \overline{k}[z'] \cdot x'^i$. On obtient une contradiction en considérant, dans les décompositions de $z'^{r-(d-3)} f = z'^r R\big(\frac{x'}{z'}, \frac{1}{z'}\big)$, les termes constants en z'. □

Soit C une courbe projective plane lisse de genre g. Le théorème de Riemann-Roch, résultat fondamental en géométrie algébrique, permet de contruire des fonctions rationnelles sur C ayant des pôles ou des zéros prescrits en certains points. Avant de l'énoncer, introduisons quelques notations.

Le groupe de Picard $\mathrm{Pic}(C)$ est le quotient de $\mathbf{Z}[C]$ par le sous-groupe $\mathrm{div}(\overline{k}(C)^*)$ des diviseurs principaux. Si D_1 et D_2 sont des diviseurs sur C, on note $D_1 \geq D_2$ lorsque pour tout $P \in C$, on a $\mathrm{ord}_P(D_1) \geq \mathrm{ord}_P(D_2)$. Pour $D \in \mathbf{Z}[C]$, on pose

$$\mathcal{L}(D) = \{f \in \overline{k}(C)^*; \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

C'est un $\overline{k}$-espace vectoriel, dont on note $\ell(D)$ la dimension (nous verrons qu'elle est finie). Cette dimension ne dépend que de la classe de D dans $\mathrm{Pic}(C)$, car $\mathcal{L}(D) = h \cdot \mathcal{L}(D + \mathrm{div}\, h)$.

Soit $\omega \in \Omega^1(\overline{k}(C))$ une forme différentielle rationnelle non nulle, et $P \in C$. Si t est une uniformisante en P, on a $\omega = f dt$ avec $f \in \overline{k}(C)^*$ (proposition 2.40). L'ordre d'annulation de f en P ne dépend pas du choix de t (si t' est une autre uniformisante, le lemme 2.42 montre que $dt' = u dt$ avec $u \in \mathcal{O}_{C,P}^*$). On note $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(f)$, et on pose alors

$$\operatorname{div}\omega = \sum_{P\in C} \operatorname{ord}_P(\omega)\cdot[P] \in \mathbf{Z}[C].$$

Montrons que cette somme est bien finie. Soit C_0 une carte affine de C. Posons $C_0 = V(F)$ avec $F \in \overline{k}[X,Y]$ irréductible. On peut supposer sans perte de généralité que $(0,0) \in C_0$ c'est-à-dire $F(0,0) = 0$. De plus, l'une des dérivées partielles de F en $(0,0)$ est non nulle, disons $\partial F/\partial Y(0,0) \neq 0$. Le raisonnement de la proposition 2.28 montre que x est une uniformisante en $(0,0)$. De plus, pour $P_0 = (x_0, y_0) \in C_0$, la fonction $x - x_0$ est une uniformisante en P_0 dès que $\partial F/\partial Y(P_0) \neq 0$; on a alors $dx = d(x - x_0)$ donc $\operatorname{ord}_{P_0}(dx) = 0$. Mais la fonction régulière $\partial F/\partial Y(x,y)$ est non nulle (sa valeur à l'origine est non nulle), donc elle ne possède qu'un nombre fini de zéros. Ainsi $\operatorname{ord}_P(dx) = 0$ sauf pour un nombre fini de $P \in C$, et comme $\omega = f dx$ avec $f \in \overline{k}(C)^*$, on a bien que $\operatorname{div}\omega$ est une somme finie.

Comme $\Omega^1(\overline{k}(C))$ est de dimension 1 sur $\overline{k}(C)$ et $\operatorname{div}(h\omega) = \operatorname{div}\omega + \operatorname{div} h$, la classe de $\operatorname{div}\omega$ dans $\operatorname{Pic}(C)$ ne dépend que de C. On l'appelle *classe canonique* et on la note K_C.

***Théorème 2.45* (Riemann-Roch).** — *Pour tout $D \in \mathbf{Z}[C]$, on a*

$$\ell(D) - \ell(K_C - D) = \deg(D) + 1 - g.$$

La démonstration de ce théorème est donnée en appendice.

Remarque 2.46. — Le fait que C est supposée plane est une restriction purement artificielle, due seulement au fait que nous n'avons pas défini les courbes algébriques en toute généralité.

Nous définissons à présent les applications rationnelles et régulières entre courbes algébriques.

Définition 2.47. — Soient C et C' des courbes affines planes. Une *application régulière* ou *morphisme* $\phi : C \to C'$ est une application dont les composantes sont des fonctions régulières sur C.

Si $\phi : C \to C'$ est un morphisme et $f \in \overline{k}[C']$ est une fonction régulière, alors $\phi^* f := f \circ \phi$ est une fonction régulière sur C, ce qui définit un morphisme de $\overline{k}$-algèbres $\phi^* : \overline{k}[C'] \to \overline{k}[C]$.

Si de plus C et C' sont irréductibles et ϕ n'est pas constante, montrons que ϕ^* est injectif. Soit $f \in \overline{k}[C']$ telle que $\phi^* f = 0$. Alors f s'annule sur $\phi(C)$. Mais $\phi(C)$ est infini : s'il n'en était pas ainsi on aurait $\phi(C) = \{Q_1, \dots, Q_n\}$ et chacun des ensembles $\{P \in C; \phi(P) = Q_i\}$ est fini car ϕ est non constante, ce qui contredit le fait que C est infini. Ainsi $f = 0$ et ϕ^* induit un morphisme de corps $\phi^* : \overline{k}(C') \to \overline{k}(C)$.

Définition 2.48. — Soient C et C' des courbes projectives planes, avec C irréductible et $C' = V(H)$. Une *application rationnelle* $\phi : C \dashrightarrow C'$ est la donnée de $\phi = (f_0 : f_1 : f_2)$ avec $f_0, f_1, f_2 \in \overline{k}(C)$ non toutes nulles et vérifiant $H(f_0, f_1, f_2) = 0$. On dit que ϕ est régulière en $P \in C$ s'il existe $g \in \overline{k}(C)^*$ telle que les $f_i' = g f_i$ soient régulières et non toutes nulles en P ; on pose alors $\phi(P) = (f_0'(P) : f_1'(P) : f_2'(P)) \in C'$.

Proposition 2.49. — *Soit $\phi : C \dashrightarrow C'$ une application rationnelle entre courbes projectives planes. On suppose que C est lisse. Alors ϕ est partout régulière.*

Démonstration. — Soit $P \in C$ et t une uniformisante en P. Posons $\phi = (f_0 : f_1 : f_2)$ et notons $m = \min(\mathrm{ord}_P(f_0), \mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2)) \in \mathbf{Z}$. Alors les fonctions rationnelles $t^{-m} f_i$ sont régulières en P et l'une d'entre elles y est non nulle, ce qui montre que ϕ est régulière en P. □

Remarque 2.50. — Soit C une courbe projective plane lisse et $\mathbf{P}^1 = V(Z)$. Si $f \in \overline{k}(C)$, on définit une application rationnelle $\widetilde{f} : C \dashrightarrow \mathbf{P}^1$ par $\widetilde{f} = (f : 1 : 0)$. D'après la proposition 2.49, $\widetilde{f}$ est partout régulière, avec $\widetilde{f}(P) = f(P)$ si f est régulière en P, et $\widetilde{f}(P) = \infty$ sinon. Les applications régulières $C \to \mathbf{P}^1$ sont ainsi en bijection avec $\overline{k}(C) \cup \{\infty\}$.

Soit $\phi : C \dashrightarrow C'$ une application rationnelle entre courbes projectives planes irréductibles. Supposons ϕ non constante. Si $f \in \overline{k}(C')$, on peut voir f comme une application rationnelle $C' \dashrightarrow \mathbf{P}^1$. La composition $f \circ \phi$ est bien définie comme application rationnelle (l'ensemble des points où f n'est pas régulière est fini, donc sa préimage par ϕ l'est aussi). On obtient ainsi un morphisme de corps $\phi^* : \overline{k}(C') \to \overline{k}(C)$. Cette extension est finie : si $f \in \overline{k}(C')$ est non constante alors $\overline{k}(\phi^* f) \subset \overline{k}(C)$ est finie (lemme 2.33), or $\overline{k}(\phi^* f) = \phi^* \overline{k}(f) \subset \phi^* \overline{k}(C')$. Le *degré* de ϕ est le degré de l'extension ϕ^*. On dit que ϕ est *séparable* si l'extension ϕ^* l'est.

Supposons de plus C, C' lisses. On sait alors que ϕ est partout régulière, induisant une application $C \to C'$. Soit $P \in C$ et $Q = \phi(P)$. Soit t_Q une uniformisante en Q. L'*indice de ramification* de ϕ en P est l'entier $e_\phi(P) = \mathrm{ord}_P(\phi^* t_Q)$. Comme $t_Q \circ \phi$ s'annule en P, on a $e_\phi(P) \geq 1$, et on vérifie que $e_\phi(P)$ ne dépend pas du choix de t_Q. Le théorème 2.35 peut alors se généraliser sous la forme suivante.

Théorème 2.51. — *Soit $\phi : C \to C'$ une application régulière non constante entre courbes projectives planes lisses. Alors*

$$\deg(\phi) = \sum_{\substack{P \in C \\ \phi(P) = Q}} e_\phi(P) \qquad (Q \in C').$$

Remarque 2.52. — Le théorème 2.35 est le cas particulier $C' = \mathbf{P}^1$, $\phi = f$ et $Q = 0$.

La démonstration du théorème 2.51 n'est pas plus difficile : il suffit de remplacer, dans la démonstration du théorème 2.35, l'anneau $A = \overline{k}[f]$ par l'anneau local $\mathcal{O}_{C',Q}$ de C' en Q, et l'idéal premier (f) de A par l'idéal maximal $\mathfrak{m}_{C',Q}$.

Théorème 2.53 **(Riemann-Hurwitz)**. — *Soient C et C' des courbes projectives planes lisses, de genres respectifs g et g'. Si $\phi : C \to C'$ est une application régulière, non constante et séparable, on a*

$$2g - 2 \geq (\deg \phi)(2g' - 2) + \sum_{P \in C} (e_\phi(P) - 1).$$

De plus, il y a égalité si aucun $e_\phi(P)$ n'est divisible par la caractéristique de k (cette condition est toujours vérifiée si $\mathrm{car}(k) = 0$).

La démonstration de ce théorème est donnée en appendice. Voici quelques applications de la formule de Riemann-Hurwitz :

(1) On a toujours $g \geq g'$ (cela découle aussi du fait que ϕ induit une application linéaire injective $\phi^* : \Omega^1(C') \to \Omega^1(C)$, voir l'appendice).

(2) Si $g' = 0$ et ϕ est non ramifié (c'est-à-dire $e_\phi(P) = 1$ pour tout $P \in C$), alors $g = 0$ et ϕ est bijectif.

(3) Si $g' = 1$ et ϕ est non ramifié, alors $g = 1$.

Exercices. — Soit k un corps et $\overline{k}$ une clôture algébrique de k.
2.1. Déterminer $\overline{k}[C]$ pour les courbes affines planes suivantes : $C = V(Y - X^2)$, $C = V(XY - 1)$ et $C = V(X^2 + Y^2 - 1)$. Les anneaux obtenus sont-ils isomorphes ?
2.2. Soit $\varphi : \mathbf{A}^1 \to \mathbf{A}^2$ définie par $t \mapsto (t^2 - 1, t^3 - t)$. Montrer que $\varphi(\mathbf{A}^1)$ est une courbe affine plane irréductible. Quels sont ses points à l'infini ?
2.3. Soit $\overline{C} = V(H)$ une courbe projective plane avec H homogène non constant sans facteur carré. Montrer que $\overline{C}$ est lisse en $(x : y : z) \in \overline{C}$ si et seulement si $(\frac{\partial H}{\partial X}, \frac{\partial H}{\partial Y}, \frac{\partial H}{\partial Z})(x, y, z) \neq (0, 0, 0)$. Si $\mathrm{car}(k) = 0$, montrer que le lieu des points singuliers de $\overline{C}$ est $V(\frac{\partial H}{\partial X}, \frac{\partial H}{\partial Y}, \frac{\partial H}{\partial Z})$.
2.4. Soit $F \in \overline{k}[X]$ qui n'est pas un carré.

(a) Montrer que la courbe $C_F = V(Y^2 - F(X))$ est irréductible.

(b) Déterminer les points à l'infini de C.

(c) À quelle condition sur F la courbe C_F (resp. $\overline{C_F}$) est-elle lisse ?

(d) Étudier de même $C_{F,d} = V(Y^d - F(X))$ et $C = V(X^n + Y^n - 1)$.

2.5. On suppose $\mathrm{car}(k) \neq 2$. Déterminer les points singuliers des courbes affines planes suivantes : $C = V(X^2 - X^4 - Y^4)$, $C = V(XY - X^6 - Y^6)$, $C = V(X^3 - Y^2 - X^4 - Y^4)$ et $C = V(X^2Y + XY^2 - X^4 - Y^4)$.
2.6. Soit C une courbe affine plane irréductible.

(a) Montrer que $\overline{k}[C]$ est factoriel si et seulement si pour tout $P \in C$, l'idéal $\mathfrak{m}_P$ est principal.

(b) On prend $C = V(Y^2 - X^3 + X)$ avec $\mathrm{car}(k) \neq 2$. Quels sont les degrés de x et y ? Déterminer $\operatorname{div} x$ et $\operatorname{div} y$.

(c) Montrer que $\mathfrak{m}_{(0,0)}$ n'est pas principal.

(d) En déduire que $\overline{k}[C]$ n'est pas factoriel et qu'il n'existe pas de fonction rationnelle de degré 1 sur C.

2.7. Soit C une courbe affine plane. Montrer que $\overline{k}[C]$ est un anneau de Dedekind si et seulement si C est irréductible et lisse.
2.8. Soit $C = V(X^3 + Y^3 - 1)$ avec $\mathrm{car}(k) \neq 3$. Déterminer le diviseur de x. Trouver une fonction rationnelle de degré 2 sur C.
2.9. Soit C une courbe projective plane irréductible et $P \in C$. Montrer qu'il existe $f \in \overline{k}(C)$ non constante et régulière sur $C - \{P\}$.

2.10. On suppose $\mathrm{car}(k) = 0$. Montrer que la droite $D = V(X+Y+Z)$ est bitangente (tangente en exactement deux points) à la quartique de Klein $C = V(X^3Y + Y^3Z + Z^3X)$. Montrer que C possède des automorphismes de la forme $(x : y : z) \mapsto (\lambda x : \mu y : \nu z)$. Pour plus d'informations, on pourra consulter [**1**].

3. Courbes elliptiques sur un corps

Soit k un corps parfait, c'est-à-dire tel que l'extension $\overline{k}/k$ soit séparable (cela revient à dire que $\mathrm{car}(k) = 0$, ou bien $\mathrm{car}(k) = p > 0$ et tout élément de k est une puissance p-ième).

A la fin du premier chapitre, nous avons donné une première définition des courbes elliptiques sur un corps (de caractéristique $\neq 2, 3$). Nous allons maintenant en donner une définition plus intrinsèque, puis montrer l'équivalence des deux définitions. Nous présentons ensuite la loi de groupe sur une courbe elliptique. La référence pour ce chapitre est [**3**, Chap. III].

Définition 3.1. — Une *courbe elliptique définie sur k* est une courbe projective plane C, définie sur k, lisse, de genre 1 et munie d'un point rationnel $O \in C(k)$.

Par exemple, la courbe de Fermat $C = V(X^3 + Y^3 - Z^3)$, munie du point rationnel $O = (1 : -1 : 0) \in C(k)$, est une courbe elliptique lorsque $\mathrm{car}(k) \neq 3$ (le genre de C vaut 1 d'après le théorème 2.44).

Théorème 3.2. — *Soit E_0 la courbe affine plane définie par*

$$E_0 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in k). \tag{4}$$

Si E_0 est non singulière, alors la complétion projective de E_0 est une courbe elliptique définie sur k.

Réciproquement, toute courbe elliptique définie sur k est isomorphe à la complétion projective d'une courbe donnée par (4).

Remarque 3.3. — On dit que (4) est une *équation de Weierstraß*. Il est important de remarquer que l'équation de Weierstraß de E_0 n'est pas unique : on peut appliquer le changement de variables affine $x = u^2x' + r$

et $y = u^3y' + u^2sx' + t$ avec $r, s, t \in k$ et $u \in k^*$. Il est possible de montrer qu'on obtient ainsi toutes les équations de Weierstraß possibles d'une courbe elliptique donnée [**3**, III.3.1(b)].

Démonstration du théorème 3.2. — Soit E_0 la courbe affine plane donnée par (4), supposée non singulière. La complétion projective E de E_0 est donnée par

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Tout point à l'infini $(x : y : 0) \in E$ vérifie $x = 0$, et donc $O := (0 : 1 : 0) \in E(k)$ est le seul point à l'infini de E_0. Dans la carte affine $Y = 1$, la courbe E devient

$$E_1 : Z + a_1XZ + a_3Z^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

et la dérivée partielle par rapport à Z montre que O est un point lisse de E. Par conséquent E est lisse. Le fait que E est de genre 1 résulte du théorème 2.44 (pour $d = 3$ on a $g = (d-1)(d-2)/2 = 1$). Ainsi E est une courbe elliptique définie sur k.

Réciproquement, donnons-nous une courbe elliptique C définie sur k, munie de $O \in C(k)$. Soit K_C un diviseur canonique sur C. En utilisant Riemann-Roch avec $D = 0$ puis $D = K_C$, on trouve $\deg K_C = 2g-2 = 0$. De plus, pour tout diviseur D sur C de degré < 0, on a $\mathcal{L}(D) = \{0\}$ car un diviseur principal est de degré 0. En utilisant le théorème de Riemann-Roch pour $D = n[O]$ avec $n \geq 1$, il vient $\ell(n[O]) - \ell(K_C - n[O]) = n$, et donc $\ell(n[O]) = n$ puisque $\deg(K_C - n[O]) < 0$. Un résultat général [**3**, II.5.8] montre que le k-espace vectoriel $\mathcal{L}(n[O]) \cap k(C)$ est de dimension $\ell(n[O])$ (ici intervient l'hypothèse que k est parfait). Comme $1 \in \mathcal{L}(2[O])$ et $\ell(2[O]) = 2$, il existe une fonction $x \in k(C)$ telle que $(1, x)$ soit une base de $\mathcal{L}(2[O])$. Alors le seul pôle de x est O, et c'est un pôle double car $\ell([O]) = 1$. De même, il existe $y \in k(C)$ telle que $(1, x, y)$ soit une base de $\mathcal{L}(3[O])$, et y admet un pôle triple en O. Alors les sept fonctions $1, x, y, x^2, xy, x^3, y^2$ appartiennent à $\mathcal{L}(6[O])$, qui est de dimension 6, donc il existe une relation de dépendance linéaire $A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0$ avec les $A_i \in k$ non tous nuls. Si $A_6 = 0$ ou $A_7 = 0$, on a une contradiction en considérant l'ordre d'annulation en

O. Ainsi A_6 et A_7 sont non nuls, et quitte à remplacer x par $-A_6A_7x$ et y par $A_6A_7^2y$, on peut supposer $A_7 = -A_6$, donc x et y satisfont une équation de la forme (4). Notons E_0 la courbe affine plane définie par cette équation, et E la complétion projective de E_0. En posant $\phi = (x : y : 1)$, on définit une application rationnelle $\phi : C \dashrightarrow E$. Puisque C est lisse, l'application ϕ est régulière (théorème 2.49), et on vérifie que $\phi(O)$ est le point à l'infini de E_0. Il reste à montrer que ϕ est un isomorphisme. Prouvons d'abord que E est lisse. On a déjà vu que le point à l'infini l'est. Supposons par l'absurde que (x_0, y_0) est un point singulier de E_0. Quitte à changer x et y en $x - x_0$ et $y - y_0$ respectivement, on peut supposer $(x_0, y_0) = (0, 0)$. Alors $a_6 = 0$ et l'examen des dérivées partielles montre que $a_3 = a_4 = 0$, donc E_0 est de la forme

$$E_0 : y^2 + a_1xy = x^3 + a_2x^2.$$

La fonction rationnelle $t = y/x$ sur C a un pôle simple en O. En reportant $y = tx$ dans l'équation précédente, il vient $t(t + a_1) = x + a_2$, donc tout pôle de t est un pôle de x, ce qui montre que O est le seul pôle de t. Mais ceci contredit le fait que $\ell([O]) = 1$ et que x et y sont linéairement indépendantes. Ainsi E est lisse. En particulier E est irréductible (théorème 2.44), et il fait sens de parler de $\phi^* : \overline{k}(E) \to \overline{k}(C)$ puisque ϕ est non constante. Comme $\deg(x) = 2$, l'extension $\overline{k}(x) \subset \overline{k}(C)$ est de degré 2 (théorème 2.35). Comme $y \notin \overline{k}(x)$ (autrement l'ordre d'annulation en O de y serait pair), il vient $\overline{k}(x, y) = \overline{k}(C)$ ce qui signifie que ϕ^* est surjectif et $\deg \phi = 1$. Mais l'isomorphisme $(\phi^*)^{-1}$ permet de définir une application rationnelle inverse $\psi : E \dashrightarrow C$, qui est régulière puisque E est lisse, et qui vérifie $\psi \circ \phi = \mathrm{id}_C$ et $\phi \circ \psi = \mathrm{id}_E$, ce qui achève de montrer que C et E sont isomorphes.

Enfin si $\mathrm{car}(k) \neq 2, 3$, les changements de variables $y' = y + (a_1x + a_3)/2$ puis $x' = x + a_2/3$ montrent que l'on peut supposer $a_1 = a_2 = a_3 = 0$. □

Remarque 3.4. — Une équation de Weierstraß de la forme $y^2 = x^3 + ax + b$ avec $a, b \in k$ est dite *réduite*.

Proposition 3.5. — *Supposons* $\mathrm{car}(k) \neq 2$. *Soit* $a, b \in k$. *La courbe affine plane* $E_0 : y^2 = x^3 + ax + b$ *est lisse si et seulement si* $\Delta := 4a^3 + 27b^2 \neq 0$. *Dans ce cas, elle définit donc une courbe elliptique.*

Démonstration. — Posons $F = Y^2 - G(X)$ avec $G(X) = X^3 + aX + b$. Supposons que E_0 possède un point singulier $P_0 = (x_0, y_0)$. Alors P_0 annule les dérivées partielles de F, ce qui donne $3x_0^2 + a = 2y_0 = 0$ et donc $y_0 = 0$ et x_0 est racine double de G. Par suite $\Delta = 0$.

Réciproquement, si $\Delta = 0$, alors G possède une racine double $x_0 \in \overline{k}$, et $P_0 = (x_0, 0)$ annule les dérivées partielles de F. Supposons par l'absurde que E_0 est lisse. Alors la complétion projective de E_0 l'est aussi, le point à l'infini étant toujours lisse. Par suite F est irréductible (théorème 2.44), et la définition 2.25 de la lissité est contredite en P_0. □

Considérons la courbe elliptique E, définie sur $k = \mathbf{Q}$, donnée par (la complétion projective de)

$$E_0 : y^2 = x^3 + 17. \tag{5}$$

Rappelons que $E(\mathbf{Q}) = E_0(\mathbf{Q}) \cup \{(0 : 1 : 0)\}$, où $E_0(\mathbf{Q})$ est l'ensemble des $(x, y) \in \mathbf{Q}^2$ solutions de (5). On a par exemple $P_1 = (-1, 4) \in E_0(\mathbf{Q})$ et $P_2 = (-2, 3) \in E_0(\mathbf{Q})$. Voici une méthode géométrique permettant de construire de nouvelles solutions de (5). La droite D reliant P_1 et P_2 a pour équation $y = x+5$. Cherchons les points d'intersection de D et E_0. Si $(x, x+5) \in E_0$ alors $x^3+17 = (x+5)^2$ ce qui mène à $x^3-x^2-10x-8 = 0$. On sait déjà que ce polynôme s'annule en -1 et -2. La considération de la somme (ou du produit) des racines montre que l'autre racine est $x = 4$, ce qui fournit le point $P_3 = (4, 9) \in E_0(\mathbf{Q})$. D'autre part, la tangente T à E_0 en P_1 admet l'équation $-3(x + 1) + 8(y - 4) = 0$. On peut paramétrer T sous la forme $(x(t), y(t)) = (-1 + 8t, 4 + 3t)$. Cherchons les points d'intersection de T et E_0. Si $(-1 + 8t, 4 + 3t) \in E_0$ alors $(8t - 1)^3 + 17 - (4 + 3t)^2 = 0$. Mais on sait déjà que ce polynôme admet $t = 0$ comme racine double (T est tangente en P_1). La troisième racine se calcule donc aisément, et on trouve $t = 201/512$, ce qui donne la solution $P_1' = (137/64, 2651/512) \in E_0(\mathbf{Q})$, beaucoup moins évidente ! Plus généralement, étant donnés deux points de $E_0(\mathbf{Q})$, la droite qui les relie a une équation rationnelle, et elle intersecte E_0 en un troisième point dont les coordonnées sont encore rationnelles. Le même résultat résultat vaut pour la tangente en un point de $E_0(\mathbf{Q})$.

Soit E une courbe elliptique sur k, munie de $O \in E(k)$. Rappelons que le groupe abélien $\mathrm{Pic}^0(E)$ est le quotient du groupe des diviseurs de degré 0 sur E, par le sous-groupe des diviseurs principaux.

Proposition 3.6. — *L'application $i_O : E \to \mathrm{Pic}^0(E)$ qui à P associe la classe du diviseur $[P] - [O]$, est bijective.*

Démonstration. — Montrons d'abord l'injectivité. Soient $P, Q \in E$ distincts tels que $i_O(P) = i_O(Q)$. Alors le diviseur $[P] - [Q]$ est principal, donc il existe $f \in \overline{k}(E)^*$ telle que $\mathrm{div}(f) = [P] - [Q]$. On a $f \in \mathcal{L}([Q])$, et comme f n'est pas constante, cela entraîne $\ell([Q]) \geq 2$. Or, comme dans la démonstration du théorème 3.2, le théorème de Riemann-Roch implique $\ell([Q]) = 1$, d'où une contradiction.

Montrons ensuite la surjectivité. Soit D un diviseur de degré 0 sur E. Toujours par le théorème de Riemann-Roch, on a $\ell(D + [O]) = 1$, d'où l'existence d'une fonction $f \in \overline{k}(E)^*$ telle que $\mathrm{div}\, f \geq -D - [O]$. Comme le degré d'un diviseur principal est nul (corollaire 2.36), on a nécessairement $\mathrm{div}\, f = -D - [O] + [P]$ avec $P \in E$, ce qui montre que la classe de D vaut $i_O(P)$. □

Par transport de structure, la bijection i_O permet de munir E d'une structure de groupe abélien, dont la loi sera notée $+$, pour laquelle O est élément neutre (puisque $i_O(O) = 0$). L'opposé d'un point $P \in E$ sera noté $-P$; c'est l'unique point Q vérifiant $P+Q = O$. On définit de même mP pour $m \in \mathbf{Z}$. Nous allons maintenant interpréter géométriquement la loi de groupe sur E.

Proposition 3.7. — *Soit D une droite projective de $\mathbf{P}^2$.*

(1) *Si D coupe E en trois points distincts P, Q, R, alors $P+Q+R = O$.*

(2) *Si D est tangente à E en P, et coupe E en un point Q distinct de P, alors $2P + Q = O$.*

(3) *Si D est tangente à E en P, et ne recoupe pas E (on dit alors que P est un* point d'inflexion de *E), alors $3P = O$.*

Démonstration. — Si D est la droite à l'infini $D_\infty = V(Z)$, alors $D_\infty \cap E = \{O\}$ et on a bien $3O = O$.

On suppose maintenant $D \neq D_\infty$, donc $D = V(\alpha X + \beta Y + \gamma Z)$ avec $(\alpha, \beta) \neq (0,0)$. Posons $f = \alpha x + \beta y + \gamma$. Le seul pôle de f est le point O. Il est au plus triple car $\mathrm{ord}_O(x) = -2$ et $\mathrm{ord}_O(y) = -3$.

Dans le cas (1), on a nécessairement $\mathrm{div}\, f = [P] + [Q] + [R] - 3[O]$ (si l'un des points P, Q, R est O alors $\beta = 0$, la droite D est verticale et $\mathrm{ord}_O(f) = -2$). Comme la classe de $\mathrm{div}\, f$ dans $\mathrm{Pic}^0(E)$ est nulle, on obtient $P + Q + R = O$.

Dans le cas (2), on a $P \neq O$ puisque $D \neq D_\infty$. Comme D est tangente en P, il vient $f \in \mathfrak{m}_P^2$, d'où $\mathrm{ord}_P(f) \geq 2$ et par suite $\mathrm{div}\, f = 2[P] + [Q] - 3[O]$. On conclut comme précédemment.

Enfin, dans le cas (3), on a $P \neq O$ et $D \cap E = \{P\}$. Puisque $\deg(f) = 3$, il vient $\mathrm{div}\, f = 3[P] - 3[O]$, d'où $3P = O$. □

Remarque 3.8. — Il suit de la démonstration précédente que dans les cas (1), (2) et (3), on a respectivement $D \cap E = \{P, Q, R\}$, $\{P, Q\}$ et $\{P\}$. De plus, il n'y a pas d'autre cas possible (considérer la forme du diviseur de f).

On peut donner des formules explicites pour la loi de groupe sur E.

Proposition 3.9. — *Soient $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ deux points de E. Le point $P_3 = P_1 + P_2$ est donné par :*

(1) *si $x_1 = x_2$ et $y_1 + y_2 + a_1 x_1 + a_3 = 0$, alors $P_3 = O$;*

(2) *sinon $P_3 = (x_3, y_3) = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \nu - a_3)$, avec*

$$(\lambda, \nu) = \begin{cases} \left(\frac{y_2 - y_1}{x_2 - x_1}, \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}\right) & \text{si } x_1 \neq x_2, \\ \left(\frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}, \frac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}\right) & \text{si } x_1 = x_2. \end{cases}$$

Démonstration. — Supposons $x_1 = x_2$ et $y_1 + y_2 + a_1 x_1 + a_3 = 0$. Si $P_1 \neq P_2$ alors la droite $x = x_1$ passe par P_1, P_2 et O donc $P_1 + P_2 = O$ par la proposition 3.7. Si $P_1 = P_2$ alors la droite $x = x_1$ est tangente à E en P_1 puisque $2y_1 + a_1 x_1 + a_3 = 0$, et l'on a encore $P_1 + P_2 = 2P_1 = O$.

Si on n'est pas dans le cas (1), alors toujours par la proposition 3.7, on a $P_3 \neq O$. Posons $P_3 = (x_3, y_3)$. Supposons d'abord $x_1 \neq x_2$ (donc $P_1 \neq P_2$). La droite D joignant P_1 et P_2 a pour équation affine $y = \lambda x + \nu$.

On sait que $D \cap E = \{P_1, P_2, -P_3\}$ et par le cas (1) on a $x(-P_3) = x(P_3) = x_3$. On trouve x_3 en reportant l'équation de D dans celle de E, ce qui donne $(\lambda x+\nu)^2+(a_1x+a_3)(\lambda x+\nu) = x^3+a_2x^2+a_4x+a_6$. Ce polynôme admet pour racines x_1, x_2, x_3 (noter qu'on peut avoir $-P_3 = P_i$, auquel cas D est tangente à E en P_i). La somme des racines vaut $\lambda^2 + a_1\lambda - a_2$, d'où la formule pour x_3. De plus, $y(-P_3) = \lambda x_3 + \nu$ et la formule pour y_3 résulte du cas (1).

Supposons enfin $x_1 = x_2$. On a nécessairement $P_1 = P_2$ car sinon la droite verticale $x = x_1$ passe par P_1, P_2 et O, d'où $P_3 = O$, impossible. On vérifie que $D : y = \lambda x+\nu$ est la tangente de E en P_1 (le dénominateur de λ est non nul car $y_1 = y_2$ et $y_1 + y_2 + a_1x_1 + a_3 \neq 0$ par hypothèse). On a $D \cap E = \{P_1, -P_3\}$ et le même argument que ci-dessus donne la formule pour x_3, puis pour y_3 (noter qu'on peut avoir $-P_3 = P_1$, auquel cas P_1 est un point d'inflexion de E). □

Remarque 3.10. — Pour une forme réduite $E : y^2 = x^3 + ax + b$, l'opposé du point (x_0, y_0) est donné par $(x_0, -y_0)$ (considérer la droite verticale $x = x_0$). Dans le cas général, l'opposé est donné par 3.9(1).

Proposition 3.11. — *Pour toute courbe elliptique E définie sur k, l'ensemble $E(k)$ est un sous-groupe de E.*

Démonstration. — Cela résulte de la proposition 3.9. □

Définition 3.12. — Pour tout entier $m \in \mathbf{Z}$, on note $[m] : E \to E$ l'application $P \mapsto mP$, définie en utilisant la structure de groupe de E.

Théorème 3.13. — *Pour tout $m \in \mathbf{Z}$, l'application $[m] : E \to E$ est régulière. De plus $[m]$ est surjective si $m \neq 0$.*

Démonstration. — L'idée est que les coordonnées de mP sont, grâce à la proposition 3.9, des fonctions rationnelles en les coordonnées de P. On utilise alors la proposition 2.49 pour conclure à la régularité de $[m]$.

Plus précisément, les formules de la proposition 3.9 montrent que $P+Q$ s'exprime rationnellement en fonction des coordonnées de P et Q, et cette expression est uniforme au moins lorsque $P, Q \neq O$ et $P \neq \pm Q$. Nous noterons $X = \{(P, Q) \in E^2; P, Q \text{ ou } P \pm Q = O\}$.

L'application $[-1] : E \to E$ est donnée par $(x, y) \mapsto (x, -y - a_1x - a_3)$. Elle est clairement rationnelle, donc régulière. Comme c'est une involution, elle est surjective.

Soit maintenant $m \in \mathbf{Z}$ quelconque. Comme $[-m] = [-1] \circ [m]$, on peut supposer $m \geq 1$. Par récurrence, il suffit d'établir le résultat suivant : si $\phi, \psi : E \to E$ sont régulières alors $\phi + \psi$ l'est aussi. Montrons-le d'abord si l'une des applications, disons ψ, est constante, égale à $Q \in E$. Dans ce cas $\phi + \psi$ est la composition $\tau_Q \circ \phi$ où $\tau_Q : P \mapsto P + Q$ est la translation par Q. Les formules explicites montrent que τ_Q est une application rationnelle (elle est définie au moins sur $E - \{O, \pm Q\}$), donc régulière, d'où la régularité de $\phi + \psi$. Soient maintenant $\phi, \psi : E \to E$ régulières quelconques. Si $\phi, \psi \neq 0$ et $\phi \neq \pm\psi$, alors l'ensemble $S = \{P \in E; (\phi(P), \psi(P)) \in X\}$ est fini ce qui fait que $\phi + \psi$ est rationnelle et définie au moins sur $E - S$; par suite, elle est régulière. Si ϕ ou ψ ou $\phi + \psi$ est nulle, le résultat est évident. Enfin, si $\phi = \psi$, on peut écrire $\phi + \phi = (\phi + (\phi + Q)) + (-Q)$ par associativité, et en choisissant $Q \neq O$ on a $\phi \neq \phi + Q$, ce qui nous ramène au cas précédent.

Il reste à montrer que $[m]$ est surjective (i.e. non constante) pour $m \geq 2$. Comme $[mn] = [m] \circ [n]$, il suffit de traiter le cas où m est premier. Commençons par le cas $m = 2$. Supposons par l'absurde $[2] = [0]$. Tout $P = (x, y) \in E$ vérifie $2P = O$ et donc $2y + a_1x + a_3 = 0$ d'après la proposition 3.9. Si $\mathrm{car}(k) \neq 2$, on trouve, en reportant dans l'équation de Weierstraß, un polynôme de degré 3 dont tout $x \in \overline{k}$ est racine, ce qui est absurde. Si $\mathrm{car}(k) = 2$, on a $a_1x + a_3 = 0$ pour tout $x \in \overline{k}$, donc $a_1 = a_3 = 0$. L'équation de E s'écrit alors $y^2 = P(x)$ avec $P(x) = x^2 + a_2x^2 + a_4x + a_6$ et $P'(x) = x^2 + a_4$. En choisissant $x_0 \in \overline{k}$ tel que $P'(x_0) = 0$ et $y_0 \in \overline{k}$ tel que $(x_0, y_0) \in E$, on obtient un point singulier de E, ce qui est absurde.

Supposons maintenant m impair et $\mathrm{car}(k) \neq 2$. On voit qu'il existe $P \neq O$ tel que $2P = O$ (considérer une racine du polynôme de degré 3 mentionné plus haut). Alors $mP = P \neq O$, donc $[m]$ est non constante.

Supposons enfin m impair et $\mathrm{car}(k) = 2$. Cherchons les $P = (x, y) \in E - \{O\}$ tels que $3P = O$. Cela équivaut à $2P = -P$, c'est-à-dire à $x(2P) = x(P)$ (puisque $2P \neq P$), ce qui est encore équivalent au système

$$\begin{cases} a_1 x + a_3 \neq 0 \\ \lambda^2 + a_1\lambda + a_2 = x \qquad \text{avec } \lambda = \frac{x^2+a_4+a_1 y}{a_1 x+a_3}. \end{cases}$$

Après calculs, la dernière équation conduit à un polynôme unitaire de degré 4 en x, dont au moins une racine vérifie $a_1 x + a_3 \neq 0$. On a ainsi montré qu'il existe $P \neq O$ tel que $3P = O$, ce qui entraîne $mP \neq O$ si $m \geq 5$. Enfin, pour $m = 3$, le calcul précédent montre qu'il existe P tel que $3P \neq O$. □

Définition 3.14. — Soient E, E' des courbes elliptiques sur k. Une *isogénie* $\phi : E \to E'$ est une application régulière vérifiant $\phi(O) = O$. On note $\mathrm{Hom}(E, E')$ l'ensemble des isogénies de E dans E'. On dit que E et E' sont *isogènes* s'il existe une isogénie non nulle $\phi : E \to E'$.

Définition 3.15. — Soit E une courbe elliptique sur k. Un *endomorphisme* de E est une isogénie de E dans E. On note $\mathrm{End}(E)$ l'ensemble des endomorphismes de E.

Exemple 3.16. — Soit E une courbe elliptique sur le corps fini $k = \mathbf{F}_q$. L'application $\phi : E \to E$ définie par $\phi(x, y) = (x^q, y^q)$ et $\phi(O) = O$ est rationnelle, donc régulière. C'est *l'endomorphisme de Frobenius* de E. En utilisant les formules explicites, on voit que ϕ est un morphisme de groupes : on a $\phi(P + Q) = \phi(P) + \phi(Q)$ pour tous $P, Q \in E$. D'autre part ϕ est bijective, puisque $x \mapsto x^q$ est une bijection de $\overline{k}$. Cependant, ce n'est pas un isomorphisme, puisque $\phi^*\overline{k}(E) = \overline{k}(E)^q \subsetneq \overline{k}(E)$. On a en fait $\deg \phi = [\overline{k}(E) : \overline{k}(E)^q] = [\overline{k}(x) : \overline{k}(x)^q]$ puisque $[\overline{k}(E) : \overline{k}(x)] = 2$, et donc $\deg \phi = q$. Enfin, on remarque que $E(\mathbf{F}_q)$ est l'ensemble des points fixes de E.

Remarque 3.17. — On montre plus généralement que toute isogénie entre courbes elliptiques est un morphisme de groupes.

Définition 3.18. — Soit E une courbe elliptique sur k, donnée par l'équation de Weierstraß (4). La *forme différentielle invariante* est

$$\omega = \frac{dx}{2y + a_1 x + a_3}. \tag{6}$$

Cela a bien un sens car on a vu que la fonction $2y + a_1x + a_3$ n'est pas identiquement nulle. En différentiant l'équation de Weierstraß, il vient aussi

$$\omega = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}. \tag{7}$$

Remarque 3.19. — En toute rigueur, on doit parler d'*une* forme différentielle invariante. En effet, le changement de variables $x = u^2x'$ et $y = u^3y'$, avec $u \in \overline{k}^*$, conduit à la forme $\omega' = dx'/(2y' + a_1'x' + a_3') = u\omega$.

Proposition 3.20. — *Le diviseur de ω est nul.*

Démonstration. — Comme E est lisse, les dérivées partielles de l'équation de Weierstraß ne s'annulent pas simultanément sur E, ce qui entraîne (via (6) et (7)) la régularité de ω sur $E - \{O\}$. Calculons l'ordre de ω en O. Comme $\mathrm{ord}_O(x) = -2$ et $\mathrm{ord}_O(y) = -3$, une uniformisante est donnée par $t = x/y$. Supposons $\mathrm{car}(k) \neq 2$. La forme différentielle $d(t^2x) = t^2dx + 2txdt$ est régulière en O, mais $\mathrm{ord}_O(txdt) = -1$, ce qui force $\mathrm{ord}_O(t^2dx) = -1$ et donc $\mathrm{ord}_O(dx) = -3$. De plus $\mathrm{ord}_O(2y + a_1x + a_3) = \mathrm{ord}_O(y) = -3$, d'où finalement $\mathrm{ord}_O(\omega) = 0$. Si $\mathrm{car}(k) = 2$, on montre de même $\mathrm{ord}_O(\omega) = 0$ en utilisant (7). Ainsi ω est régulière sur E. Or nous avons vu que $\deg(\mathrm{div}\,\omega) = \deg K_C = 0$, ce qui impose $\mathrm{div}\,\omega = 0$. □

Pour toute application régulière non constante $\phi : E \to E'$ entre courbes elliptiques, rappelons qu'on dispose de $\phi^* : \overline{k}(E') \to \overline{k}(E)$, qui induit une application $\phi^* : \Omega^1(\overline{k}(E')) \to \Omega^1(\overline{k}(E))$.

Proposition 3.21. — *La forme différentielle ω est invariante par translation : pour tout $Q \in E$, on a $\tau_Q^*\omega = \omega$, avec $\tau_Q : P \mapsto P + Q$.*

Démonstration. — Le diviseur de $\tau_Q^*\omega$ est le translaté (par $-Q$) du diviseur de ω, qui est nul d'après la proposition 3.20. En particulier $\tau_Q^*\omega$ est régulière sur E et donc $\tau_Q^*\omega = \lambda_Q\omega$ avec $\lambda_Q \in \overline{k}^*$. En utilisant la formule explicite pour l'addition sur E, on s'aperçoit que $Q \mapsto \lambda_Q$ est une fonction rationnelle sur E. Comme elle est régulière partout, elle est nécessairement constante, et donc $\lambda_Q = \lambda_O = 1$ pour tout $Q \in E$. □

Exemple 3.22. — Soit Λ un réseau de $\mathbf{C}$. On a vu au chapitre 1 que $\mathbf{C}/\Lambda$ est en bijection avec une courbe elliptique E définie sur $\mathbf{C}$. Notons $\phi : \mathbf{C}/\Lambda \to E$ cette bijection. On a un diagramme commutatif

$$\begin{array}{ccc} \mathbf{C}/\Lambda & \xrightarrow{\phi} & E \\ \cong\downarrow & & \downarrow\cong \\ \mathrm{Pic}^0(\mathbf{C}/\Lambda) & \xrightarrow{\phi_*} & \mathrm{Pic}^0(E) \end{array}$$

où ϕ_* envoie $\sum n_i[z_i]$ sur $\sum n_i[\phi(z_i)]$. Ce diagramme montre que ϕ est un isomorphisme de groupes. On peut calculer l'image réciproque par ϕ de la forme différentielle invariante $\omega = dx/y$. Comme $\phi(z) = (\wp(z), \wp'(z))$, il vient $\phi^*\omega = d(\wp(z))/\wp'(z) = dz$. On constate que la forme différentielle holomorphe dz sur $\mathbf{C}/\Lambda$ est bien invariante par translation (c'est la seule, à multiplication près par un nombre complexe).

Exercices. — **3.1.** Soit E la courbe elliptique sur $\mathbf{Q}$ définie par $y^2 = x^3 + 17$. On pose $P_1 = (-1, 4)$, $P_2 = (-2, 3)$ et $P_3 = (4, 9) \in E(\mathbf{Q})$.

(a) Calculer $P_2 - P_1$, $2P_2$ et $2P_2 + P_1$.

(b) En considérant des points de la forme $mP_1 + nP_2$ avec $m, n \in \mathbf{Z}$, trouver deux autres couples $(x, y) \in \mathbf{N}^2$ vérifiant $y^2 = x^3 + 17$.

3.2. Pour chacune des courbes suivantes, montrer que E est une courbe elliptique sur $\mathbf{F}_5$, faire la liste des points de $E(\mathbf{F}_5)$ et déterminer la structure de ce groupe :

(a) $E : y^2 = x^3 + x$;

(b) $E : y^2 = x^3 + 2x$;

(c) $E : y^2 = x^3 + 1$.

3.3. Soit $C = V(X^3 + Y^3 + Z^3 + dXYZ)$ avec $d \in k$ ($\mathrm{car}(k) \neq 3$).

(a) Montrer que C est lisse si et seulement si $d^3 \neq -1$.

(b) On suppose désormais que C est lisse. Montrer que C est une courbe elliptique sur k.

(c) Soit $P = (x_0 : x_1 : x_2) \in C$. Montrer que la tangente de C en P recoupe la courbe au point $Q = (y_0 : y_1 : y_2)$ donné par $y_i = x_i(x_{i+1}^3 - x_{i+2}^3)$, où les indices sont pris modulo 3.

(d) Soient $P = (x_0 : x_1 : x_2)$ et $Q = (y_0 : y_1 : y_2)$ des points distincts de C. Montrer que la droite joignant P et Q recoupe C au point $R = (z_0 : z_1 : z_2)$ donné par $z_i = x_i^2 y_{i+1} y_{i+2} - y_i^2 x_{i+1} x_{i+2}$ (formules de Desboves).

(e) On prend $C = V(X^3 + Y^3 + 7Z^3)$. En partant du point $(2 : -1 : -1)$, trouver dix points de $C(\mathbf{Q})$.

3.4. On considère la courbe de Fermat $C = V(X^3 + Y^3 - Z^3)$ avec $\mathrm{car}(k) \neq 2, 3$, munie de $O = (1 : -1 : 0) \in C(k)$.

(a) Déterminer l'équation la tangente T de C en O.

(b) En déduire que O est un point d'inflexion de C.

(c) Avec une transformation projective envoyant T sur la droite à l'infini, mettre C sous forme de Weierstraß (on explicitera l'isomorphisme).

(d) Déterminer les droites projectives D passant par O, distinctes de T, qui sont tangentes à C.

(e) En déduire les points d'ordre 2 de C. Vérifier ce résultat en utilisant l'équation de Weierstraß.

(f) Déterminer les points $P \in C$ vérifiant $3P = O$.

4. Courbes elliptiques sur les corps finis et locaux

Soit E une courbe elliptique définie sur le corps fini $\mathbf{F}_q$ à q éléments. L'ensemble $E(\mathbf{F}_q)$ est un groupe abélien fini. Une estimation de son cardinal est donnée par le théorème suivant, démontré par Hasse vers 1930.

Théorème 4.1. — *On a l'inégalité* $|\operatorname{card} E(\mathbf{F}_q) - q - 1| \leq 2\sqrt{q}$.

Remarque 4.2. — Si l'on choisit une équation de Weierstraß pour E, une estimation grossière donne $\operatorname{card} E(\mathbf{F}_q) \leq 2q+1$: pour chaque $x \in \mathbf{F}_q$, au plus deux $y \in \mathbf{F}_q$ vérifient l'équation. Le nombre de racines d'un polynôme de degré 2 dans $\mathbf{F}_q$ avec q impair est $0, 1$ ou 2, suivant que le discriminant est ou n'est pas un carré. On peut donc s'attendre à environ q points dans $E(\mathbf{F}_q)$, ce que confirme le théorème de Hasse.

Par ailleurs, Deuring a montré que si q est premier, la borne de Hasse est optimale : pour $a \in \mathbf{Z}$ avec $|a| \leq 2\sqrt{q}$, il existe une courbe elliptique E vérifiant $\operatorname{card} E(\mathbf{F}_q) = q + 1 - a$. Il donne même le nombre de telles courbes elliptiques : c'est le nombre de classes de Kronecker de $a^2 - 4q$.

Démonstration. — Soit $\phi : (x, y) \mapsto (x^q, y^q)$ l'endomorphisme de Frobenius de E. Pour $P \in E$, on a $P \in E(\mathbf{F}_q)$ si et seulement si $\phi(P) = P$, ce qui s'écrit aussi $E(\mathbf{F}_q) = \ker(1 - \phi)$. L'isogénie $1 - \phi$ est non constante.

La première étape consite à montrer que $1 - \phi$ est séparable. Soit $\omega \in \Omega^1(\overline{\mathbf{F}_q}(E))$ la forme différentielle invariante sur E. L'application $F : (P, Q) \mapsto P - \phi(Q)$ s'exprime rationnellement en termes de P et Q, et cette expression est uniforme pour $P, Q \neq 0$ et $P \neq \pm\phi(Q)$. On peut considérer $F^*\omega = \omega \circ F$, qui est une forme différentielle rationnelle en $x(P), y(P), x(Q), y(Q)$. Comme les coordonnées de Q interviennent à la puissance q dans $F(P, Q)$, les différentielles $dx(Q)$ et $dy(Q)$ disparaissent dans $F^*\omega$, ce qui donne $F^*\omega = f(P, Q)\omega(P)$ où $f(P, Q)$ est une fonction rationnelle de P et Q, et $\omega(P)$ est obtenu à partir de ω en remplaçant (x, y) par $(x(P), y(P))$. Si l'on fixe $Q_0 \in E$ et l'on note τ la translation par $-\phi(Q_0)$, on a $F(P, Q_0) = \tau(P)$ d'où $f(P, Q_0)\omega(P) = \tau^*\omega = \omega$, ce qui montre que $f(P, Q_0) = 1$ comme fonction rationnelle en P. Ceci étant vrai pour tout $Q_0 \in E$, on a $f = 1$ d'où $F^*\omega = \omega(P)$. Mais $(1 - \phi)(P) = F(P, P)$, on a donc $(1 - \phi)^*\omega = \omega$ et par suite $(1 - \phi)^*$ est injective sur $\Omega^1(\overline{\mathbf{F}_q}(E))$.

Soit t une uniformisante en $O \in E$ et $u = (1-\phi)^*t$. On sait que $dt \neq 0$ (théorème 2.40) et donc $du = (1 - \phi)^*dt \neq 0$. Soit $f \in \overline{\mathbf{F}_q}(E)$. Montrons que f est séparable sur $\overline{\mathbf{F}_q}(u)$. Si ce n'est pas le cas alors le polynôme minimal de f s'écrit $\mu = X^{pn} + a_{n-1}X^{p(n-1)} + \cdots + a_1X^p + a_0$ avec $a_i \in \overline{\mathbf{F}_q}(u)$. En dérivant $\mu(f) = 0$, il vient $\sum_{i=0}^{n-1} a_i' f^{p(n-1)} = 0$ en notant $da_i = a_i' du$. Pour tout i, cela entraîne $a_i' = 0$ et donc a_i est une puissance p-ième. Mais on obtient alors un polynôme de degré n annulant f, ce qui contredit la minimalité du degré de μ. Ainsi tout élément de $\overline{\mathbf{F}_q}(E)$ est séparable sur $\overline{\mathbf{F}_q}(u) = (1 - \phi)^*\overline{\mathbf{F}_q}(t)$, donc a fortiori sur $(1 - \phi)^*\overline{\mathbf{F}_q}(E)$.

En appliquant Riemann-Hurwitz à l'isogénie $1 - \phi : E \to E$, on obtient que $e_{1-\phi}(P) = 1$ pour tout $P \in E$, c'est-à-dire que $1 - \phi$ est non ramifiée. Par le théorème 2.51 appliqué en $Q = O$, on a donc $\operatorname{card} E(\mathbf{F}_q) = \operatorname{card} \ker(1 - \phi) = \deg(1 - \phi)$.

La seconde étape est de montrer que $Q(m, n) = \deg(m + n\phi)$ est une forme quadratique sur $\mathbf{Z}^2$ (par convention on pose $\deg[0] = 0$). Admettons ce point. Comme Q est positive, l'inégalité de Cauchy-Schwarz

donne $|\deg(1-\phi)-\deg(1)-\deg(\phi)| \leq 2\sqrt{\deg(1)\deg(\phi)}$ c'est-à-dire $|\operatorname{card} E(\mathbf{F}_q)-q-1| \leq 2\sqrt{q}$.

Lemme 4.3. — *Soit $\psi : E \to E$ une isogénie de degré $m \geq 1$. Il existe une unique isogénie $\widehat{\psi}$, appelée isogénie duale de ψ, telle que $\widehat{\psi}\circ\psi = \psi\circ\widehat{\psi} = [m]$.*

Montrons l'unicité. Si $\widehat{\psi}'$ vérifie la même chose, alors $(\widehat{\psi}'-\widehat{\psi})\circ\psi = [m]-[m] = 0$ et comme ψ est surjective, il vient $\widehat{\psi}' = \widehat{\psi}$.

Pour l'existence, supposons d'abord ψ séparable. On a vu que dans ce cas $\operatorname{card}\ker\psi = \deg(\psi) = m$ donc $\ker\psi \subset \ker[m]$. Pour tout $P \in E$, la translation τ_P induit un automorphisme de $\overline{\mathbf{F}_q}(E)$. Considérons le groupe fini d'automorphismes $G = \{\tau_P ; P \in \ker\psi\}$. Pour des raisons de degré, le corps $\psi^*\overline{\mathbf{F}_q}(E)$ s'identifie au corps fixe $\overline{\mathbf{F}_q}(E)^G$. Comme tout élément de G fixe $[m]^*\overline{\mathbf{F}_q}(E)$, on a $[m]^*\overline{\mathbf{F}_q}(E) \subset \psi^*\overline{\mathbf{F}_q}(E)$, ce qui permet de définir un endomorphisme λ^* du corps $\overline{\mathbf{F}_q}(E)$, fixant $\overline{\mathbf{F}_q}$, tel que $[m]^* = \psi^*\circ\lambda^*$. Les fonctions rationnelles λ^*x et λ^*y permettent de définir une application rationnelle $\widehat{\psi} : E \dashrightarrow E$ telle que $\widehat{\psi}^* = \lambda^*$. Alors $\widehat{\psi}$ est régulière et vérifie $\widehat{\psi}\circ\psi = [m]$. Comme $\psi\circ\widehat{\psi}\circ\psi = \psi\circ[m] = [m]\circ\psi$, on a aussi $\psi\circ\widehat{\psi} = [m]$.

Supposons maintenant ψ non séparable. Soit K la fermeture séparable de $\psi^*\overline{\mathbf{F}_q}(E)$ dans $\overline{\mathbf{F}_q}(E)$. Le degré q' de l'extension $K \subset \overline{\mathbf{F}_q}(E)$ est une puissance de la caractéristique p de $\mathbf{F}_q$. Comme cette extension est purement inséparable, on a $\overline{\mathbf{F}_q}(E)^{q'} \subset K$. Comme $[\overline{\mathbf{F}_q}(E) : \overline{\mathbf{F}_q}(E)^{q'}] = q'$, l'inclusion est une égalité et on en tire $\psi^*\overline{\mathbf{F}_q}(E) \subset \overline{\mathbf{F}_q}(E)^{q'}$. Soit E' la courbe elliptique sur $\mathbf{F}_q$ obtenue en élevant tous les coefficients de l'équation de Weierstraß de E à la puissance q'. L'application $\phi' : (x,y) \mapsto (x^{q'}, y^{q'})$ définit une isogénie $E \to E'$, et l'on a $(\phi')^*\overline{\mathbf{F}_q}(E) = \overline{\mathbf{F}_q}(E)^{q'}$. Par un raisonnement analogue au paragraphe précédent, l'isogénie ψ se factorise en $\psi = \chi\circ\phi'$, où χ est une isogénie séparable $E' \to E$. Comme le cas séparable a déjà été traité et $\deg(\psi) = \deg(\chi)\deg(\phi')$, on est ramenés à montrer que ϕ' admet une isogénie duale. Quitte à composer les isogénies duales, on peut aussi supposer $q' = p$. Par une méthode analogue à celle employée pour montrer $(1-\phi)^*\omega = \omega$, on montre par récurrence sur $n \geq 1$ que $[n]^*\omega = n\omega$ et donc $[p]^*\omega = 0$. Par l'absurde, supposons l'isogénie $[p] : E \to E$ séparable. Soit t une uniformisante en $O \in E$. Puisque $\overline{\mathbf{F}_q}([p]^*t) \subset [p]^*\overline{\mathbf{F}_q}(E)$ est séparable, il en va de

même de $\overline{\mathbf{F}_q}([p]^*t) \subset \overline{\mathbf{F}_q}(E)$ et l'on sait alors que $[p]^*dt = d([p]^*t) \neq 0$ (démonstration de la proposition 2.40), ce qui contredit $[p]^*\omega = 0$. Ainsi $[p] : E \to E$ se factorise en $[p] = \chi \circ \phi''$ avec une isogénie $\phi'' : E \to E''$ qui se factorise au moins par ϕ', ce qui achève de montrer le lemme 4.3.

Une propriété fondamentale des isogénies duales est que $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$ [**3**, III.§6.2(c)]. Par une récurrence immédiate, on en déduit $\widehat{[m]} = m\widehat{[1]} = [m]$ pour $m \in \mathbf{Z}$. En posant $d = \deg[m]$, il vient $[d] = \widehat{[m]} \circ [m] = [m^2]$ ce qui montre que $\deg[m] = m^2$ (il existe une démonstration directe, mais très calculatoire, de ce fait important).

On peut maintenant achever la démonstration du théorème de Hasse. En calculant dans $\mathbf{Z} \subset \mathrm{End}(E)$, il vient

$$\begin{aligned} Q(m,n) &= (m + n\phi) \circ (\widehat{m + n\phi}) \\ &= m^2 + n^2(\phi \circ \widehat{\phi}) + mn(\phi + \widehat{\phi}) \\ &= m^2 + qn^2 + mn(\phi + \widehat{\phi}) \end{aligned}$$

donc Q est une forme quadratique sur $\mathbf{Z}^2$. □

Pour $m \in \mathbf{Z}$, on note $E[m]$ le noyau de l'isogénie $[m] : E \to E$.

Proposition 4.4. — *Soit E une courbe elliptique sur $\mathbf{F}_q$, et notons p la caractéristique de $\mathbf{F}_q$.*

(1) *Si p ne divise pas $m \in \mathbf{Z}$ alors $E[m] \cong \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$.*

(2) *On a l'alternative suivante : ou bien $E[p^r] \cong \mathbf{Z}/p^r\mathbf{Z}$ pour tout $r \geq 1$, ou bien $E[p^r] = 0$ pour tout $r \geq 1$.*

Démonstration. — (1) Soit $m \geq 2$ non divisible par p. On a $[m]^*\omega = m\omega \neq 0$ donc $[m]$ est séparable. Il en résulte $\mathrm{card}\, E[m] = \deg[m] = m^2$. De même $\mathrm{card}\, E[d] = d^2$ pour tout d divisant m. Posons $E[m] \cong \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}$ avec $n_1 \geq 2$ et $n_i | n_{i+1}$. Alors n_r divise m, et comme $E[m] = E[n_r]$ est de cardinal n_r^2, il vient $n_r = m$. De plus $n_1^2 = \mathrm{card}\, E[n_1] = n_1^r$ donc $r = 2$ et $n_1 = m$.

(2) Soit E' la courbe elliptique sur $\mathbf{F}_q$ obtenue à partir de E en élevant les coefficients de l'équation de Weierstraß à la puissance p. Notons $\phi' : E \to E'$ l'isogénie définie par $(x, y) \mapsto (x^p, y^p)$. On a vu que

$[p] = \chi \circ \phi'$ où $\chi : E' \to E$ est une isogénie. En prenant les degrés, il vient $p^2 = \deg(\chi)\deg(\phi') = p\deg(\chi)$ car $(\phi')^*\overline{\mathbf{F}_q}(E') = \overline{\mathbf{F}_q}(E)^p$. Ainsi $\deg(\chi) = p$. Comme ϕ' est bijectif, on a $\operatorname{card} E[p] = \operatorname{card}\ker\chi$. Si χ est séparable, ce cardinal vaut p, auquel cas $E[p] \cong \mathbf{Z}/p\mathbf{Z}$. Par récurrence et par surjectivité de $[p]$, on a alors $\operatorname{card} E[p^r] = p^r$ et $E[p^r]$ possède un point d'ordre p^r, donc $E[p^r] \cong \mathbf{Z}/p^r\mathbf{Z}$. Enfin si χ n'est pas séparable, les propriétés de factorisation des isogénies montrent que χ est un Frobenius $E' \to E''$ (cela montre au passage que $E \cong E''$ peut être définie sur $\mathbf{F}_{p^2}$) donc $[p]$ est bijectif et $E[p^r] = 0$ pour tout r.

□

Remarque 4.5. — Lorsque $E[p] = 0$, on dit que E est *supersingulière* (ne pas confondre avec la notion de singularité définie pour les courbes algébriques). On peut alors montrer que $\mathrm{End}(E)$ est un $\mathbf{Z}$-module libre de rang 4 (c'est un ordre dans une algèbre de quaternions). Lorsque $E[p] \cong \mathbf{Z}/p\mathbf{Z}$, on dit que E est *ordinaire* ; dans ce cas $\mathrm{End}(E)$ est un $\mathbf{Z}$-module libre de rang 2 (c'est un ordre dans un corps quadratique imaginaire).

Donnons, sans démonstration, l'énoncé de l'hypothèse de Riemann pour une courbe elliptique E sur $\mathbf{F}_q$. La *fonction zêta de* E est

$$Z(E,T) = \exp\Big(\sum_{n\geq 1} \operatorname{card} E(\mathbf{F}_{q^n}) \cdot \frac{T^n}{n}\Big) \in \mathbf{Q}[[T]]. \tag{8}$$

Elle encode le nombre de points de E sur toutes les extensions finies de $\mathbf{F}_q$. Posons $\operatorname{card} E(\mathbf{F}_q) = q + 1 - a$ avec $a \in \mathbf{Z}$.

***Théorème 4.6* (Weil)**. — *On a l'identité*

$$Z(E,T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}. \tag{9}$$

Remarque 4.7. — Expliquons en quoi cette identité est l'analogue de l'hypothèse de Riemann. D'après $|a| \leq 2\sqrt{q}$, il vient $1 - aT + qT^2 = (1-\alpha T)(1-\overline{\alpha}T)$ avec $\alpha \in \mathbf{C}$, $|\alpha| = \sqrt{q}$. En posant $\zeta_E(s) = Z(E, q^{-s})$ pour $s \in \mathbf{C}$, on vérifie facilement l'équation fonctionnelle $\zeta_E(1-s) = \zeta_E(s)$ et le fait que $\zeta_E(s) = 0$ entraîne $\Re(s) = \frac{1}{2}$.

Nous allons maintenant étudier les courbes elliptiques sur les corps locaux. Soit p un nombre premier. Notons $|\cdot|_p$ (resp. v_p) la norme (resp. valuation) p-adique sur $\mathbf{Q}_p$, de sorte que $|x|_p = p^{-v_p(x)}$ pour tout $x \in \mathbf{Q}_p$. Rappelons que $\mathbf{Z}_p = \{x \in \mathbf{Q}_p; v_p(x) \geq 0\}$ et que $\mathbf{Z}_p/p\mathbf{Z}_p \cong \mathbf{F}_p$.

Soit E une courbe elliptique sur $\mathbf{Q}_p$. D'après le théorème 3.2, la courbe E possède une équation de Weierstraß

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in \mathbf{Q}_p). \tag{10}$$

Le *discriminant* Δ de cette équation est donné par les formules suivantes

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned}$$

Le discriminant d'une équation de Weierstraß est non nul si et seulement si cette équation définit une courbe elliptique. Pour une équation réduite $y^2 = x^3 + ax + b$, on a la formule plus simple $\Delta = -16(4a^3 + 27b^2)$. Un long calcul montre que le changement de variables le plus général, à savoir $x = u^2x' + r$ et $y = u^3y' + u^2sx' + t$ avec $u \neq 0$, résulte en le discriminant $\Delta' = u^{-12}\Delta$.

Le changement de variables $x = u^{-2}x'$, $y = u^{-3}y'$ avec $u \in \mathbf{Q}_p^*$ conduit à une autre équation de Weierstraß dont les coefficients a_i' sont donnés par $a_i' = u^ia_i$. En prenant $v_p(u)$ suffisamment grand, on a alors $a_i' \in \mathbf{Z}_p$ pour tout i, et donc E possède une équation de Weierstraß à coefficients dans $\mathbf{Z}_p$. On a alors, en particulier, $\Delta \in \mathbf{Z}_p$, $\Delta \neq 0$.

Définition 4.8. — Une équation de Weierstraß (10) est dite *minimale* pour E en p si les deux conditions suivantes sont vérifiées :

(a) $a_i \in \mathbf{Z}_p$ pour tout i ;

(b) $v_p(\Delta)$ est minimal parmi toutes les équations de Weierstraß de E à coefficients dans $\mathbf{Z}_p$.

Remarque 4.9. — L'existence d'une équation minimale pour E résulte du fait que $v_p(\Delta) \in \mathbf{N}$. De plus, comme le discriminant est multiplié par une puissance douzième lors d'un changement de variables, toute équation de Weierstraß avec $a_i \in \mathbf{Z}_p$ et $v_p(\Delta) < 12$ est minimale en p.

Toute équation de Weierstraß vérifiant $a_i \in \mathbf{Z}_p$ peut être réduite modulo p, définissant une courbe projective plane sur $\mathbf{F}_p$.

Proposition 4.10. — *Soit E une courbe elliptique sur $\mathbf{Q}_p$. La réduction modulo p d'une équation de Weierstraß minimale pour E en p ne dépend pas de l'équation minimale choisie.*

Démonstration. — Donnons-nous deux équations de Weierstraß minimales pour E, de coefficients a_i et a_i'. Elles sont reliées par un changement de variables $x = u^2x' + r$ et $y = u^3y' + u^2sx' + t$ avec $r, s, t, u \in \mathbf{Q}_p$, $u \neq 0$. Il suffit de montrer que $r, s, t \in \mathbf{Z}_p$ et $u \in \mathbf{Z}_p^*$. En effet, on aura $\overline{u} \in \mathbf{F}_p^*$ et la réduction modulo p du changement de variables définira alors un isomorphisme entre les deux réductions modulo p de E.

Comme $\Delta = u^{12}\Delta'$ et $v_p(\Delta) = v_p(\Delta')$, on a $u \in \mathbf{Z}_p^*$. Après calculs, on a également les formules de transformation suivantes

$$\begin{aligned}
u^2b_2' &= b_2 + 12r \\
u^4b_4' &= b_4 + rb_2 + 6r^2 \\
u^6b_6' &= b_6 + 2rb_4 + r^2b_2 + 4r^3 \\
u^8b_8' &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4
\end{aligned}$$

et l'on sait que $b_j, b_j' \in \mathbf{Z}_p$. La formule pour b_2' donne $12r \in \mathbf{Z}_p$. Si $p \neq 2, 3$, on en déduit $r \in \mathbf{Z}_p$.

Supposons $p = 3$. Alors $v_3(r) \geq -1$. Supposons par l'absurde $v_3(r) = -1$. Dans la formule pour b_6', on a $v_3(b_6 + 2rb_4 + r^2b_2) \geq -2$ et $v_3(4r^3) = -3$, ce qui est absurde car $b_6' \in \mathbf{Z}_3$. Donc $r \in \mathbf{Z}_3$.

Supposons $p = 2$. On a $v_2(r) \geq -2$. En raisonnant de même avec la formule pour b_8', on a $v_2(b_8 + 3rb_6 + 3r^2b_4 + r^3b_2) \geq 3v_2(r)$ et $v_2(3r^4) = 4v_2(r)$, ce qui entraîne $r \in \mathbf{Z}_2$.

Dans tous les cas, on a donc $r \in \mathbf{Z}_p$. De plus, la formule $u^2 a'_2 = a_2 - sa_1 + 3r - s^2$ entraîne $s \in \mathbf{Z}_p$. Enfin, la formule $u^6 a'_6 = a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1$ implique $t \in \mathbf{Z}_p$. □

Définition 4.11. — La *réduction* $\widetilde{E}$ *de* E *modulo* p est la courbe projective plane, définie sur $\mathbf{F}_p$, obtenue en réduisant modulo p une équation de Weierstraß minimale pour E en p.

Définition 4.12. — Soit E une courbe elliptique sur $\mathbf{Q}_p$. On dit que E a *bonne réduction en* p si sa réduction $\widetilde{E}$ modulo p est une courbe non singulière (ce qui équivaut à $\Delta \not\equiv 0 \pmod{p}$).

Remarque 4.13. — Ces définitions s'étendent aux courbes elliptiques sur $\mathbf{Q}$, qui sont de manière naturelle des courbes elliptiques sur $\mathbf{Q}_p$.

Si $P = (x : y : z) \in \mathbf{P}^2(\mathbf{Q}_p)$, il existe $u \in \mathbf{Q}_p^*$ avec $ux, uy, uz \in \mathbf{Z}_p$ et au moins l'un d'entre eux dans $\mathbf{Z}_p^*$, ce qui permet de définir $\widetilde{P} = (\overline{ux} : \overline{uy} : \overline{uz}) \in \mathbf{P}^2(\mathbf{F}_p)$, qui ne dépend pas de u. On vérifie que si $P \in E(\mathbf{Q}_p)$ alors $\widetilde{P} \in \widetilde{E}(\mathbf{F}_p)$, d'où *l'application de réduction modulo* p

$$\begin{aligned} \pi : E(\mathbf{Q}_p) &\to \widetilde{E}(\mathbf{F}_p) \\ P &\mapsto \widetilde{P}. \end{aligned}$$

Remarquons que $\widetilde{O}$ est le point à l'infini de $\widetilde{E}$. On note $\widetilde{E}_{\mathrm{ns}}$ (resp. $\widetilde{E}_{\mathrm{ns}}(\mathbf{F}_p)$) l'ensemble des points lisses de $\widetilde{E}$ (resp. $\widetilde{E}(\mathbf{F}_p)$).

Définition 4.14. — On pose $E_0(\mathbf{Q}_p) = \{P \in E(\mathbf{Q}_p); \widetilde{P} \in \widetilde{E}_{\mathrm{ns}}(\mathbf{F}_p)\}$ et $E_1(\mathbf{Q}_p) = \{P \in E(\mathbf{Q}_p); \widetilde{P} = \widetilde{O}\}$.

Proposition 4.15. — *On a une suite exacte de groupes abéliens*

$$0 \to E_1(\mathbf{Q}_p) \to E_0(\mathbf{Q}_p) \xrightarrow{\pi} \widetilde{E}_{\mathrm{ns}}(\mathbf{F}_p) \to 0. \tag{11}$$

Démonstration. — Supposons d'abord $\widetilde{E}$ non singulière. Alors $E_0(\mathbf{Q}_p) = E(\mathbf{Q}_p)$ et comme π envoie une droite de $\mathbf{P}^2(\mathbf{Q}_p)$ sur une droite de $\mathbf{P}^2(\mathbf{F}_p)$, l'application $\pi : E(\mathbf{Q}_p) \to \widetilde{E}(\mathbf{F}_p)$ est un morphisme de groupes. Par définition, son noyau est $E_1(\mathbf{Q}_p)$. Il reste à établir la surjectivité de π, qui va résulter du lemme de Hensel. Soit $F = Y^2 + a_1XY + a_3Y - X^3 -$

$a_2X^2 - a_4X - a_6 \in \mathbf{Z}_p[X,Y]$ et $\overline{F} \in \mathbf{F}_p[X,Y]$ la réduction de F modulo p. Soit $Q = (a,b) \in \widetilde{E}(\mathbf{F}_p)$. Comme Q est lisse, on sait que l'une des dérivées partielles, disons $\partial\overline{F}/\partial X(Q)$, est non nulle. Soit $y \in \mathbf{Z}_p$ tel que $\overline{y} = b$. Considérons le polynôme $P(X) = F(X,y) \in \mathbf{Z}_p[X]$. Choisissons $x_0 \in \mathbf{Z}_p$ tel que $\overline{x_0} = a$. Alors $|P(x_0)|_p < 1$ et $|P'(x_0)|_p = 1$. Le lemme de Hensel entraîne l'existence de $x \in \mathbf{Z}_p$ tel que $P(x) = 0$, ce qui fournit un point $P = (x,y) \in E(\mathbf{Q}_p)$ tel que $\widetilde{P} = Q$.

Supposons maintenant que $\widetilde{E}$ est singulière. On va montrer qu'il existe une unique structure de groupe sur $\widetilde{E}_{\mathrm{ns}}$ telle que $\widetilde{O}$ est l'élément neutre de $\widetilde{E}_{\mathrm{ns}}$ et $\widetilde{E}_{\mathrm{ns}}$ vérifie la proposition 3.7. Quitte à faire une translation dans le plan affine, on peut supposer que le point singulier de $\widetilde{E}$ est $(0,0)$. Soit $s \in \overline{\mathbf{F}_p}$ tel que $s^2 + a_1 s - a_2 = 0$. Quitte à remplacer y par $y + sx$ (ce qui est une transformation affine, donc projective), on peut supposer $a_2 = 0$, d'où $\widetilde{E} : y^2 + axy = x^3$. On vérifie alors (en distinguant les cas $p = 2$ ou 3) que $(0,0)$ est le seul point singulier de $\widetilde{E}$.

S $a \neq 0$, le changement de variables projectif $X = a^2(X' - Y')$, $Y = a^3Y'$ et $Z = Z'$ conduit à l'équation $X'Y'Z' = (X' - Y')^3$ pour $\widetilde{E}$, qui dans la carte $Y' = 1$ s'écrit $x'z' = (x' - 1)^3$. La partie non singulière $\widetilde{E}_{\mathrm{ns}}$ est incluse dans cette carte, et on a une bijection $t : \widetilde{E}_{\mathrm{ns}} \to \overline{\mathbf{F}_p}^*$ envoyant (x', z') sur x' (remarquons que $\widetilde{O}$ est envoyé sur 1). De plus, donnons-nous trois points $P, Q, R \in \widetilde{E}_{\mathrm{ns}}$ et une droite projective L évitant le point singulier. Alors L admet une équation affine de la forme $z' = \alpha x' + \beta$. Par conséquent, dire que $L \cap E = \{P, Q, R\}$ signifie que le polynôme $x'(\alpha x' + \beta) = (x' - 1)^3$ admet pour racines $t(P), t(Q), t(R)$. En regardant le terme constant, il vient $t(P)t(Q)t(R) = 1$. Réciproquement, si $t(P)t(Q)t(R) = 1$ alors il existe une droite projective L telle que $L \cap E = \{P, Q, R\}$. Par transport de structure du groupe multiplicatif via t, on obtient la structure de groupe voulue sur $\widetilde{E}_{\mathrm{ns}}$.

Si $a = 0$, alors $\widetilde{E} : y^2 = x^3$ et on a de même une bijection $t : \widetilde{E}_{\mathrm{ns}} \to \overline{\mathbf{F}_p}$ envoyant $(x,y) \neq (0,0)$ sur x/y et $\widetilde{O}$ sur 0. L'équation homogène de $\widetilde{E}_{\mathrm{ns}}$ est $Y^2Z = X^3$ ce qui, dans la carte $Y = 1$, s'écrit $z = x^3$. On voit alors que trois points $P, Q, R \in \widetilde{E}_{\mathrm{ns}}$ sont alignés si et seulement si $t(P) + t(Q) + t(R) = 0$, ce qui montre que $\widetilde{E}_{\mathrm{ns}}$ est isomorphe au groupe additif $\overline{\mathbf{F}_p}$.

Dans chacun de ces cas, $\widetilde{E}_{\mathrm{ns}}(\mathbf{F}_p)$ est un sous-groupe de $\widetilde{E}_{\mathrm{ns}}$ (une droite passant par deux points $\mathbf{F}_p$-rationnels admet une équation dans $\mathbf{F}_p$), et π est un morphisme de groupes d'après le caractère géométrique de la loi de groupe. Enfin, la surjectivité de π dans la suite (11) procède du même argument que dans le cas non singulier. □

Proposition 4.16. — *Le groupe $E_0(\mathbf{Q}_p)$ est d'indice fini dans $E(\mathbf{Q}_p)$.*

Démonstration. — Le plan projectif $\mathbf{P}^2(\mathbf{Q}_p)$ est muni d'une topologie naturelle, quotient de la topologie de $\mathbf{Q}_p^3 - \{0\}$. Il est compact car s'écrit comme la réunion de trois cartes affines homéomorphes à $\mathbf{Z}_p^2$. Comme $E(\mathbf{Q}_p)$ est fermé dans $\mathbf{P}^2(\mathbf{Q}_p)$, il est compact. De plus, toute translation $\tau : E(\mathbf{Q}_p) \to E(\mathbf{Q}_p)$ est régulière partout, a fortiori continue ; c'est donc un homéomorphisme. Tout ensemble de la forme $\pi^{-1}(Q)$, avec $Q \in \widetilde{E}(\mathbf{F}_p)$, est ouvert dans $E(\mathbf{Q}_p)$, donc $E_0(\mathbf{Q}_p)$ est un ouvert non vide de $E(\mathbf{Q}_p)$. Par suite un nombre fini de translatés de $E_0(\mathbf{Q}_p)$ recouvrent $E(\mathbf{Q}_p)$, ce qui montre que $E_0(\mathbf{Q}_p)$ est d'indice fini dans $E(\mathbf{Q}_p)$. □

Proposition 4.17. — *Si m est un entier non divisible par p, alors $E_1(\mathbf{Q}_p)[m] = 0$.*

Démonstration. — Rappelons que $E_1(\mathbf{Q}_p)[m]$ désigne le noyau de $[m]$. Si $P = (x, y) \in E_1(\mathbf{Q}_p)$ alors par définition de $\widetilde{P}$, il vient $v_p(y) \leq -1$ et $v_p(y) < v_p(x)$. Si $x \in \mathbf{Z}_p$ alors $y^2 + a_1xy + a_3y \in \mathbf{Z}_p$, ce qui est impossible. Par suite $v_p(x) \leq -1$ et $v_p(x^3 + a_2x^2 + a_4x + a_6) = 3v_p(x)$. D'autre part $v_p(y^2 + a_1xy + a_3y) = 2v_p(y)$. L'égalité $3v_p(x) = 2v_p(y)$ mène à $v_p(x) = -2n$ et $v_p(y) = -3n$ avec $n \geq 1$. Réciproquement si $P = (x, y) \in E(\mathbf{Q}_p)$ vérifie $v_p(x) \leq -2$ et $v_p(y) \leq -3$ alors $\widetilde{P} = \widetilde{O}$ donc $P \in E_1(\mathbf{Q}_p)$. Nous sommes ainsi conduits à introduire les ensembles

$$E_n(\mathbf{Q}_p) = \{(x, y) \in E(\mathbf{Q}_p); v_p(x) \leq -2n, v_p(y) \leq -3n\} \cup \{O\}.$$

Pour $n = 1$, c'est l'ensemble déjà construit. Nous allons voir que $E_n(\mathbf{Q}_p)$ est un sous-groupe de $E(\mathbf{Q}_p)$ pour tout $n \geq 1$. Partant de notre équation minimale, le changement de variables $x = p^{-2n}x'$ et $y = p^{-3n}y'$ conduit à une équation de Weierstraß à coefficients dans $\mathbf{Z}_p$, et dont la réduction

modulo p est donnée par $\widetilde{E}_n : y'^2 = x'^3$. De plus, on a une application de réduction modulo p, que nous noterons $\pi_n : E(\mathbf{Q}_p) \to \widetilde{E}_n(\mathbf{F}_p)$. Déterminons la préimage du point singulier de $\widetilde{E}_n$. Si $P = (x, y) \in E(\mathbf{Q}_p)$ vérifie $\pi_n(P) = (0, 0)$ alors $v_p(x'), v_p(y') \geq 1$ donc $v_p(x) > -2n$ et $v_p(y) > -3n$, et donc $P \notin E_n(\mathbf{Q}_p)$. Réciproquement si $P = (x, y) \notin E_n(\mathbf{Q}_p)$ alors $v_p(x')$ ou $v_p(y')$ est ≥ 1 et donc $\pi_n(P) = (0, 0)$. Ainsi $E_n(\mathbf{Q}_p)$ est la préimage par π_n de la partie non singulière de $E_n(\mathbf{Q}_p)$, dont on a par ailleurs vu qu'elle est isomorphe au groupe additif $\mathbf{F}_p$. Donc $E_n(\mathbf{Q}_p)$ est un sous-groupe de $E(\mathbf{Q}_p)$ et on a un morphisme surjectif $\pi_n : E_n(\mathbf{Q}_p) \to \mathbf{F}_p$. Enfin, déterminons le noyau de ce morphisme. Si $P = (x, y) \in E_n(\mathbf{Q}_p)$ est tel que $\pi_n(P)$ est le point à l'infini de $\widetilde{E}_n$, alors $v_p(y') \leq -1$ c'est-à-dire $v_p(y) \leq -3n - 1$. Mais l'analyse du début de la démonstration montre que dans ce cas $P \in E_{n+1}(\mathbf{Q}_p)$. Réciproquement si $P \in E_{n+1}(\mathbf{Q}_p)$ alors $\pi_n(P) = \widetilde{O}$. Pour résumer, on a une suite exacte de groupes abéliens

$$0 \to E_{n+1}(\mathbf{Q}_p) \to E_n(\mathbf{Q}_p) \xrightarrow{\pi_n} \mathbf{F}_p \to 0.$$

Soit maintenant $P \in E_1(\mathbf{Q}_p)$ tel que $[m]P = O$. Alors $m\pi_1(P) = \pi_1([m]P) = 0$ et comme m est premier à p, il vient $\pi_1(P) = 0$ c'est-à-dire $P \in E_2(\mathbf{Q}_p)$. Par une récurrence immédiate, on a $P \in E_n(\mathbf{Q}_p)$ pour tout $n \geq 1$. Puisque $\cap_{n \geq 1} E_n(\mathbf{Q}_p) = \{O\}$, il vient finalement $P = O$. □

Corollaire 4.18. — *Soit E une courbe elliptique sur $\mathbf{Q}_p$ ayant bonne réduction en p. Si m est un entier non divisible par p, alors l'application de réduction $E(\mathbf{Q}_p)[m] \to \widetilde{E}(\mathbf{F}_p)$ est injective.*

Démonstration. — Si E a bonne réduction en p alors $E_0(\mathbf{Q}_p) = E(\mathbf{Q}_p)$ et $\widetilde{E}_{\mathrm{ns}}(\mathbf{F}_p) = \widetilde{E}(\mathbf{F}_p)$. Comme le noyau de la réduction $E(\mathbf{Q}_p) \to \widetilde{E}(\mathbf{F}_p)$ est par définition $E_1(\mathbf{Q}_p)$, la proposition 4.17 permet de conclure. □

Noter que si E est une courbe elliptique définie sur $\mathbf{Q}$, on a une injection naturelle $E(\mathbf{Q}) \subset E(\mathbf{Q}_p)$. Le corollaire 4.18 fournit donc des informations intéressantes pour déterminer les points de torsion de $E(\mathbf{Q})$.

Exemple 4.19. — Soit E la courbe elliptique sur $\mathbf{Q}$ d'équation $y^2 + y = x^3$. On vérifie que $\Delta = -27$ donc cette équation est minimale en p pour tout nombre premier p. De plus E a bonne réduction en p pour $p \neq 3$.

Déterminons les points de $E(\mathbf{Q})$ d'ordre $m \geq 2$. Si m est impair, on peut utiliser le corollaire 4.18 avec $p = 2$, d'où une injection $E(\mathbf{Q})[m] \hookrightarrow \widetilde{E}(\mathbf{F}_2)$. On voit facilement $\operatorname{card} \widetilde{E}(\mathbf{F}_2) = 3$ d'où $E(\mathbf{Q})[m] \hookrightarrow \mathbf{Z}/3\mathbf{Z}$. Par suite, si $P \in E(\mathbf{Q})$ est un point d'ordre m impair, on a nécessairement $m = 3$ et il y a au plus deux points d'ordre 3. Réciproquement, les points $P_1 = (0, 0)$ et $P_2 = (0, -1)$ sont d'ordre 3 (la tangente en P_1 est la droite $y = 0$, qui coupe E seulement en P_1, donc P_1 est un point d'inflexion ; de même pour P_2). Pour $m = 2$, on voit à la main que $E(\mathbf{Q})[2] = 0$ (résoudre $P = -P$) donc $E(\mathbf{Q})$ n'a pas d'élément d'ordre 2^n si $n \geq 1$. Finalement, les points de torsion de $E(\mathbf{Q})$ sont $\{O, P_1, P_2\}$. D'autres exemples sont donnés en exercice.

Exercices. — **4.1.** Soit p un nombre premier vérifiant $p \equiv 2 \pmod 3$. Soit E une courbe elliptique sur $\mathbf{F}_p$ de la forme $E : y^2 = x^3 + D$ avec $D \in \mathbf{F}_p^*$. Montrer que $\operatorname{card} E(\mathbf{F}_p) = p + 1$.

4.2. Soit p un nombre premier vérifiant $p \equiv 3 \pmod 4$. Soit E une courbe elliptique sur $\mathbf{F}_p$ de la forme $E : y^2 = x^3 + Dx$ avec $D \in \mathbf{F}_p^*$. Montrer que $\operatorname{card} E(\mathbf{F}_p) = p+1$ (on pourra remarquer que parmi les éléments $x^3 + Dx$ et $-x^3 - Dx$, supposés non nuls, l'un est un carré et l'autre non).

4.3. Soient E_1, E_2 deux courbes elliptiques sur $\mathbf{F}_q$. On suppose qu'il existe une isogénie $\psi : E_1 \to E_2$ non nulle et définie sur $\mathbf{F}_q$. Montrer que $\operatorname{card} E_1(\mathbf{F}_q) = \operatorname{card} E_2(\mathbf{F}_q)$ (on pourra utiliser $1 - \phi_1$ et $1 - \phi_2$).

4.4. Déterminer les points de torsion de $E(\mathbf{Q})$ pour les courbes elliptiques définies sur $\mathbf{Q}$ suivantes :

(a) $E : y^2 = x^3 + 1$

(b) $E : y^2 = x(x - 1)(x + 2)$

(c) $E : y^2 = x(x + 1)(x + 4)$

(d) $E : y^2 = x^3 - 43x + 166$

5. Points rationnels

Le but de ce chapitre est de démontrer le théorème suivant.

***Théorème* (Mordell, 1922)**. — *Pour toute courbe elliptique E définie sur $\mathbf{Q}$, le groupe abélien $E(\mathbf{Q})$ est de type fini.*

Remarque 5.1. — Le théorème de structure des groupes abéliens de type fini donne alors un isomorphisme (non canonique)

$$E(\mathbf{Q}) \cong E(\mathbf{Q})_{\mathrm{tors}} \times \mathbf{Z}^r$$

où $E(\mathbf{Q})_{\mathrm{tors}}$ est le *sous-groupe de torsion* de $E(\mathbf{Q})$, qui est donc fini, et r est le *rang* de E. Le fait que $E(\mathbf{Q})_{\mathrm{tors}}$ est fini peut se démontrer uniquement à l'aide du chapitre précédent : en effet, il suffit de choisir deux nombres premiers $p \neq q$ en lesquels E a bonne réduction, et de remarquer, grâce au corollaire 4.18, que la torsion de $E(\mathbf{Q})$ d'ordre premier à p (resp. q) s'injecte dans un groupe fini ; ainsi $E(\mathbf{Q})_{\mathrm{tors}}$ est fini.

Remarque 5.2. — Le théorème de Mordell a été généralisé par Weil aux variétés abéliennes (donc aux courbes elliptiques) définies sur les corps de nombres, d'où le nom courant de théorème de Mordell-Weil. Plus généralement encore, Néron a montré que si A est une variété abélienne définie sur un corps K qui est de type fini sur $\mathbf{Q}$ ou $\mathbf{F}_p$ (suivant la caractéristique de K), alors $A(K)$ est de type fini.

La preuve du théorème de Mordell s'effectue en deux étapes. On commence par montrer une version faible : le groupe $E(\mathbf{Q})/2E(\mathbf{Q})$ est fini. On utilise ensuite un procédé de descente, où il s'agit de montrer que les points de $E(\mathbf{Q})$ ne peuvent être indéfiniment divisibles par 2.

Pour la première étape, montrons le résultat général suivant.

Théorème 5.3. — *Pour toute courbe elliptique E définie sur un corps de nombres K et tout entier $m \geq 2$, le groupe $E(K)/mE(K)$ est fini.*

Nous noterons $G_K = \mathrm{Gal}(\overline{K}/K)$ le groupe des K-automorphismes de $\overline{K}$. Une extension éventuellement infinie L/K (avec toujours $L \subset \overline{K}$) est dite galoisienne si elle est stable par G_K. Dans ce cas G_L est un sous-groupe distingué de G_K, et le groupe $\mathrm{Gal}(L/K)$ des K-automorphismes de L s'identifie au groupe quotient G_K/G_L. On obtient ainsi une bijection entre les extensions galoisiennes de K et les sous-groupes distingués de G_K, la bijection réciproque étant donnée par $H \mapsto \overline{K}^H$. Notons que G_K agit sur $E(\overline{K})$ et préserve la loi de groupe, avec $E(K) = E(\overline{K})^{G_K}$.

Lemme 5.4. — *Soit L/K une extension finie galoisienne et $m \geq 2$. Si $E(L)/mE(L)$ est fini, alors il en est de même pour $E(K)/mE(K)$.*

Démonstration. — Il s'agit de montrer que le noyau N de l'application naturelle $E(K)/mE(K) \to E(L)/mE(L)$ est fini. Pour tout $P \in N$, choisissons un représentant $\widetilde{P} \in E(K)$. Comme $P \in N$, on peut poser $\widetilde{P} = m\widetilde{Q}$ avec $\widetilde{Q} \in E(L)$. Définissons $\lambda_P : \mathrm{Gal}(L/K) \to E[m]$ par $\lambda_P(\sigma) = \sigma(\widetilde{Q}) - \widetilde{Q}$ (on a bien $m\lambda_P(\sigma) = \sigma(\widetilde{P}) - \widetilde{P} = 0$).

Montrons que l'application $P \mapsto \lambda_P$ est injective. Soient $P, P' \in N$ tels que $\lambda_P = \lambda_{P'}$. Alors $\sigma(\widetilde{Q}) - \widetilde{Q} = \sigma(\widetilde{Q'}) - \widetilde{Q'}$ pour tout σ, et donc $\widetilde{Q} - \widetilde{Q'}$ est fixé par $\mathrm{Gal}(L/K)$, ce qui entraîne $\widetilde{P} \equiv \widetilde{P'} \pmod{mE(K)}$. On conclut en remarquant qu'il n'y a qu'un nombre fini d'applications de $\mathrm{Gal}(L/K)$ dans $E[m]$. □

Comme $E[m]$ est stable par G_K, le corps K' engendré par les coordonnées des points de $E[m]$ est une extension finie galoisienne de K. Par le lemme précédent, il suffit de montrer que $E(K')/mE(K')$ est fini, avec l'avantage que $E[m] \subset E(K')$. On peut donc supposer $E[m] \subset E(K)$, ce que nous ferons par la suite.

Pour tout $P \in E(K)$ et $\sigma \in G_K$, choisissons $Q \in E(\overline{K})$ tel que $mQ = P$. Alors le point $\lambda(P, \sigma) = \sigma(Q) - Q$ ne dépend pas du choix de Q (d'après l'hypothèse $E[m] \subset E(K)$), et l'on a $m\lambda(P, \sigma) = 0$. Cela permet de définir *l'accouplement de Kummer*

$$\lambda : E(K) \times G_K \to E[m].$$

L'expression $\lambda(P, \sigma)$ est linéaire en P et l'on a

$$\lambda(P, \sigma\tau) = \sigma(\tau(Q) - Q) + (\sigma(Q) - Q) = \lambda(P, \tau) + \lambda(P, \sigma).$$

Notons L l'extension (éventuellement infinie) de K engendrée par les coordonnées des points $Q \in E(\overline{K})$ vérifiant $mQ \in E(K)$. Cette extension est galoisienne.

Lemme 5.5. — *L'accouplement de Kummer induit des injections*

$$E(K)/mE(K) \to \mathrm{Hom}(\mathrm{Gal}(L/K), E[m])$$
$$\mathrm{Gal}(L/K) \to \mathrm{Hom}(E(K), E[m]).$$

Démonstration. — Par définition de L, l'application λ annule $E(K) \times G_L$, donc induit des morphismes $\phi : E(K) \to \mathrm{Hom}(\mathrm{Gal}(L/K), E[m])$ et $\psi : \mathrm{Gal}(L/K) \to \mathrm{Hom}(E(K), E[m])$.

Montrons que $\ker \phi = mE(K)$. Si $P = mQ \in mE(K)$ alors $\lambda(P, \sigma) = 0$ pour tout σ et donc $\phi(P) = 0$. Réciproquement, soit $P \in E(K)$ tel que $\phi(P) = 0$. Alors $P = mQ$ avec $Q \in E(L)$ fixe par $\mathrm{Gal}(L/K)$, donc $Q \in E(K)$.

Montrons que ψ est injectif. Soit $\sigma \in \mathrm{Gal}(L/K)$ tel que $\psi(\sigma) = 0$. Alors pour tout point $Q \in E(L)$ tel que $mQ \in E(K)$, on a $\sigma(Q) = Q$. Comme L est engendrée par les coordonnées de tels points, on a $\sigma = 1$. □

D'après le lemme précédent, la finitude de $E(K)/mE(K)$ est équivalente à celle de l'extension L/K. On sait déjà que le groupe $\mathrm{Gal}(L/K)$ est abélien et que l'ordre de tout élément divise m. Quitte à augmenter K (c'est possible grâce au lemme 5.4), on peut aussi supposer $\zeta_m \in K$. Rappelons la structure des extensions de Kummer : si K'/K est une extension finie galoisienne de corps de nombres, avec $\zeta_m \in K$ et $\mathrm{Gal}(K'/K) \cong \mathbf{Z}/m\mathbf{Z}$, alors il existe $y \in K$ tel que $K' = K(\sqrt[m]{y})$. Cette théorie s'étend aisément aux extensions infinies, et permet de montrer le lemme suivant.

Lemme 5.6. — *L'extension L/K est engendrée par une famille (éventuellement infinie) $\sqrt[m]{y_i}$, avec $y_i \in K$.*

Démonstration. — Il suffit de montrer le résultat pour une extension finie galoisienne K'/K, avec $K' \subset L$. Or dans ce cas, $G = \mathrm{Gal}(K'/K)$ est un quotient de $\mathrm{Gal}(L/K)$, donc est abélien fini d'exposant divisant m. On a donc $G \cong \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_s\mathbf{Z}$ avec $d_i | m$. En particulier K'/K est engendrée par des extensions cycliques $K_1, \ldots, K_s$ de degrés respectifs $d_1, \ldots, d_s$. Mais le résultat est clair pour chacune de ces extensions. □

On dit que E a bonne réduction en un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ s'il existe une équation de Weierstraß pour E à coefficients dans $\mathcal{O}_K$ dont la réduction modulo $\mathfrak{p}$ soit non singulière (sur $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$). Un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ est dit non ramifié dans L si pour toute sous-extension finie $K \subset K' \subset L$, il est non ramifié dans K'.

Lemme 5.7. — *Si E a bonne réduction en $\mathfrak{p}$ ne divisant pas m, alors l'extension L/K est non ramifiée en $\mathfrak{p}$.*

Démonstration. — Par définition de L, il suffit de montrer le résultat pour l'extension K'/K engendrée par les coordonnées d'un point $Q \in E(\overline{K})$ tel que $mQ \in E(K)$. Remarquons que K'/K est finie galoisienne car $\sigma(Q)-Q \in E[m] \subset E(K)$ pour tout $\sigma \in G_K$. Soit $\mathfrak{q}$ un idéal premier de $\mathcal{O}_{K'}$ au-dessus de $\mathfrak{p}$. Alors E a bonne réduction en $\mathfrak{q}$ (on prend la même équation de Weierstraß), et en posant $k_\mathfrak{q} = \mathcal{O}_{K'}/\mathfrak{q}$, on a un morphisme de réduction $E(K') \to \widetilde{E}(k_\mathfrak{q})$. Soit $I_\mathfrak{q} \subset \mathrm{Gal}(K'/K)$ le sous-groupe d'inertie de $\mathfrak{q}$. Si $\sigma \in I_\mathfrak{q}$ alors par définition de l'inertie, Q et $\sigma(Q)$ ont même réduction modulo $\mathfrak{q}$. Le fait que $\sigma(Q) - Q \in E[m]$ et le corollaire 4.18 (étendu aux corps de nombres) impliquent alors $\sigma(Q) = Q$. Comme Q engendre K'/K, on a donc $I_\mathfrak{q} = 1$ et K'/K est non ramifiée en $\mathfrak{q}$. □

Pour $x \in K^*$, notons $x\mathcal{O}_K = \prod_\mathfrak{p} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x)}$ la décomposition de l'idéal fractionnaire $x\mathcal{O}_K$ en idéaux premiers, avec $\mathrm{ord}_\mathfrak{p}(x) \in \mathbf{Z}$. Supposons $K' = K(\sqrt[m]{y}) \subset L$ avec $y \in K^*$. Si K'/K est non ramifiée en $\mathfrak{p}$, alors $\mathfrak{p}\mathcal{O}_{K'}$ est produit d'idéaux premiers distincts, et donc pour tout $\mathfrak{q}$ au-dessus de $\mathfrak{p}$, on a $\mathrm{ord}_\mathfrak{p}(y) = \mathrm{ord}_\mathfrak{q}(y) \equiv 0 \pmod m$ puisque $\sqrt[m]{y} \in K'$.

Notons S l'ensemble des idéaux premiers de $\mathcal{O}_K$ qui divisent m, ou en lesquels E a mauvaise réduction. L'ensemble S est fini (si l'on prend n'importe quelle équation de Weierstraß pour E à coefficients dans $\mathcal{O}_K$, son discriminant n'est divisible que par un nombre fini d'idéaux premiers). Le paragraphe précédent nous amène à considérer l'ensemble

$$T = \{y \in K^*/(K^*)^m ; \mathrm{ord}_\mathfrak{p}(y) \equiv 0 \pmod m \text{ si } \mathfrak{p} \notin S\}.$$

D'après tout ce qu'on a dit, l'extension L/K est engendrée par les racines m-ièmes de certains éléments de T. Nous allons voir en fait que T est fini.

Considérons le sous-anneau $\mathcal{O}_K[\frac{1}{S}] = \{x \in K ; \mathrm{ord}_\mathfrak{p}(x) \geq 0 \text{ si } \mathfrak{p} \notin S\}$. Comme le nombre de classes de $\mathcal{O}_K$ est fini, l'anneau $\mathcal{O}_K$ devient principal après avoir inversé un nombre fini d'idéaux premiers. Quitte à augmenter S (ce qui ne fait qu'augmenter T), on peut donc supposer que $\mathcal{O}_K[\frac{1}{S}]$ est principal. Montrons que l'application naturelle $\mathcal{O}_K[\frac{1}{S}]^* \to T$ est surjective. Elle est bien définie car $\mathrm{ord}_\mathfrak{p}(x) = 0$ pour $x \in \mathcal{O}_K[\frac{1}{S}]^*$ et $\mathfrak{p} \notin S$. Soit $y \in K^*$ représentant un élément de T. Alors $y\mathcal{O}_K[\frac{1}{S}]$ est la puissance m-ième d'un idéal nécessairement principal $z\mathcal{O}_K[\frac{1}{S}]$, d'où $y = z^m u$ avec

$u \in \mathcal{O}_K[\frac{1}{S}]^*$, et donc y et u représentent le même élément de T. D'après le théorème des unités de Dirichlet, le groupe $\mathcal{O}_K[\frac{1}{S}]^*$ est de type fini. Donc T est de type fini et de torsion, et par conséquent fini. Cela achève de montrer le théorème 5.3.

Remarque 5.8. — Pour montrer la finitude de L/K, on peut aussi faire appel au théorème d'Hermite-Minkowski : il n'existe qu'un nombre fini de corps de nombres de degré donné et non ramifiés en dehors d'un ensemble fini fixé de nombres premiers. En effet L/K est engendrée par des extensions de degré $\leq m$ et non ramifiées en dehors de S. Comme il n'y a qu'un nombre fini de telles extensions, on en déduit que L/K est finie.

Passons à la seconde partie de la démonstration du théorème de Mordell. Nous supposons maintenant que E est une courbe elliptique définie sur $\mathbf{Q}$. Il existe une équation de Weierstraß pour E de la forme $y^2 = x^3 + ax + b$ avec $a, b \in \mathbf{Z}$. Il s'agit d'analyser en détail la multiplication par 2 sur $E(\mathbf{Q})$. On voit sur des exemples (ou par la formule) qu'étant donné un point P dans $E(\mathbf{Q})$, le point $2P$ est en général "plus compliqué". Pour quantifier cette observation, on introduit la *hauteur* d'un nombre rationnel.

Définition 5.9. — Pour $x = u/v \in \mathbf{Q}$ avec $u, v \in \mathbf{Z}$ premiers entre eux, on pose $H(x) = \max(|u|, |v|)$ et $h(x) = \log H(x) \geq 0$.

En première approximation, on peut dire que la hauteur $h(x)$ est proportionnelle à la quantité d'encre nécessaire pour écrire x explicitement.

Définition 5.10. — La *hauteur* $h : E(\mathbf{Q}) \to \mathbf{R}$ est donnée par

$$h(P) = \begin{cases} h(x) & \text{si } P = (x, y) \neq O \\ 0 & \text{si } P = O. \end{cases}$$

Bien sûr, cette hauteur dépend de l'équation de Weierstraß choisie.

Lemme 5.11. — *Pour tout C, l'ensemble $\{P \in E(\mathbf{Q}); h(P) \leq C\}$ est fini.*

Démonstration. — Il n'y a qu'un nombre fini de $x \in \mathbf{Q}$ vérifiant $h(x) \leq C$, et chaque x donne lieu à au plus deux points de $E(\mathbf{Q})$. □

Lemme 5.12. — *Soit $P_0 \in E(\mathbf{Q})$. Il existe C telle que pour tout $P \in E(\mathbf{Q})$ on ait $h(P+P_0) \leq 2h(P) + C$.*

Démonstration. — Le résultat est trivial pour $P_0 = O$. En prenant $C \geq \max(h(P_0), h(2P_0))$, on peut supposer $P \neq O, \pm P_0$. Posant $P_0 = (x_0, y_0)$ et $P = (x, y)$, la formule d'addition donne

$$\begin{aligned} x(P+P_0) &= \Big(\frac{y-y_0}{x-x_0}\Big)^2 - x - x_0 \\ &= \frac{x^3 + ax + b + x_0^3 + ax_0 + b - 2yy_0 - (x+x_0)(x-x_0)^2}{(x-x_0)^2} \\ &= \frac{(x+x_0)(xx_0+a) + 2b - 2yy_0}{(x-x_0)^2}. \end{aligned}$$

D'après la forme de l'équation de Weierstraß, on a nécessairement $x = u/w^2$ et $y = v/w^3$ avec u, w (resp. v, w) entiers premiers entre eux. Posons aussi $x_0 = u_0/w_0^2$ et $y_0 = v_0/w_0^3$. En multipliant numérateur et dénominateur de $x(P+P_0)$ par $w^4 w_0^4$, on obtient

$$x(P+P_0) = \frac{(uw_0^2 + u_0 w^2)(uu_0 + aw^2 w_0^2) + 2bw^4 w_0^4 - 2vv_0 ww_0}{(uw_0^2 - u_0 w^2)^2} =: \frac{A}{B}.$$

D'après cette écriture (et même si la fraction est réductible), il vient $H(x(P+P_0)) \leq \max(|A|, |B|)$ et il suffit de majorer A et B. On a d'une part $|B| \leq C_1 \max(u^2, w^4) \leq C_1 H(x)^2$, et d'autre part $|A| \leq C_2 \max(u^2, w^4, |vw|)$, où les constantes C_i ne dépendent pas de P. Comme P est sur la courbe, il vient $v^2 = u^3 + auw^4 + bw^6$ d'où

$$|vw| \leq C_3 \max(|u|^{3/2}|w|, |u|^{1/2}|w|^3, |w|^4) \leq C_3 H(x)^2.$$

On obtient l'inégalité désirée en passant au logarithme. □

Le résultat suivant est crucial dans la preuve du théorème de Mordell.

Lemme 5.13. — *Il existe C' telle que pour tout $P \in E(\mathbf{Q})$ on ait $h(2P) \geq 4h(P) - C'$.*

Démonstration. — Quitte à augmenter C'', on peut supposer $2P \neq O$. En posant $P = (x, y)$ il vient alors

$$\begin{aligned} x(2P) &= \Big(\frac{3x^2+a}{2y}\Big)^2 - 2x \\ &= \frac{9x^4 + 6ax^2 + a^2 - 8x(x^3+ax+b)}{4(x^3+ax+b)} \\ &= \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3+ax+b)}. \end{aligned}$$

En appliquant l'algorithme d'Euclide à $F = X^4 - 2aX^2 - 8bX + a^2$ et $G = X^3 + aX + b$, on constate que ces polynômes sont premiers entre eux dans $\mathbf{Q}[X]$. Plus précisément, posant $\Delta = 4a^3 + 27b^2 \neq 0$, on trouve des polynômes $F_1, G_1 \in \mathbf{Z}[X]$ de degrés respectifs 2 et 3 tels que $F_1F + G_1G = \Delta$. En appliquant l'algorithme aux polynômes réciproques de F et G (définis par $\widetilde{F} = X^4F(1/X)$ et $\widetilde{G} = X^3G(1/X)$), on trouve également $F_2, G_2 \in \mathbf{Z}[X]$ de degrés respectifs 3 et ≤ 3 tels que $F_2F + G_2G = \Delta \cdot X^7$.

Posons $x = u/v$ avec $u, v \in \mathbf{Z}$ premiers entre eux. Alors $x(2P) = A/B$ avec $A = v^4F(u/v) \in \mathbf{Z}$ et $B = 4v^4G(u/v) \in \mathbf{Z}$. Soit $\delta = \mathrm{pgcd}(A, B)$. Comme $4v \cdot v^2F_1(u/v) \cdot A + v^3G_1(u/v) \cdot B = 4v^7\Delta$, on a $\delta | 4v^7\Delta$. De même $4 \cdot v^3F_2(u/v) \cdot A + v^3G_2(u/v) \cdot B = 4u^7\Delta$ entraîne $\delta | 4u^7\Delta$ et finalement $\delta | 4\Delta$. Par suite $H(x(2P)) \geq \max(|A|, |B|)/|4\Delta|$.

Si R est un polynôme de $\mathbf{Z}[X]$ de degré $\leq d$, alors $|v^dR(u/v)| \leq C_0 \max(|u|^d, |v|^d)$ où la constante C_0 ne dépend que des coefficients de R. En appliquant ce principe aux identités ci-dessus, il vient

$$\begin{aligned} |4v^7\Delta| &\leq C_1 \max(|u|^3, |v|^3) \cdot \max(|A|, |B|) \\ |4u^7\Delta| &\leq C_2 \max(|u|^3, |v|^3) \cdot \max(|A|, |B|). \end{aligned}$$

On en déduit $|4\Delta| H(x)^7 \leq C_3 H(x)^3 \cdot \max(|A|, |B|)$. Par suite $H(x(2P)) \geq H(x)^4/C_3$ ce qui s'écrit aussi $h(2P) \geq 4h(P) - C'$. □

Démonstration du théorème de Mordell. — D'après le théorème 5.3, le groupe $E(\mathbf{Q})/2E(\mathbf{Q})$ est fini. Choisissons un système de représentants $Q_1, \ldots, Q_s$ de $E(\mathbf{Q})/2E(\mathbf{Q})$ dans $E(\mathbf{Q})$.

Soit $P \in E(\mathbf{Q})$. On a $P = Q_{i_1} + 2P_1$ avec $1 \leq i_1 \leq s$ et $P_1 \in E(\mathbf{Q})$. En continuant ainsi, on construit une suite P_n de points de $E(\mathbf{Q})$ telle que $P_n = Q_{i_{n+1}} + 2P_{n+1}$ pour tout n. On a

$$\begin{aligned} h(P_{n+1}) &\leq \frac{1}{4}\big(h(2P_{n+1}) + C'\big) \\ &\leq \frac{1}{4}\big(h(P_n - Q_{i_{n+1}}) + C'\big) \\ &\leq \frac{1}{4}\big(2h(P_n) + C + C'\big) \end{aligned}$$

où l'on a pris une constante C telle que le lemme 5.12 est vérifié pour tout $P_0 \in \{-Q_1, \ldots, -Q_s\}$. Par une récurrence immédiate, on a

$$h(P_n) \leq h(P)/2^n + (C + C')/2$$

pour tout n. Par suite, il existe une constante C'' (par exemple $C'' = 1 + (C + C')/2$) telle que pour n suffisamment grand, on ait $h(P_n) \leq C''$. On en déduit que P appartient au sous-groupe de $E(\mathbf{Q})$ engendré par les $Q_1, \ldots, Q_s$ et l'ensemble fini $\{Q \in E(\mathbf{Q}); h(Q) \leq C''\}$. On a donc bien montré que $E(\mathbf{Q})$ est de type fini. □

Remarque 5.14. — On peut se demander, étant donnée une courbe elliptique E sur $\mathbf{Q}$, s'il existe un algorithme pour obtenir un système de générateurs de $E(\mathbf{Q})$. Un examen de la preuve ci-dessus montre qu'il suffirait de trouver des générateurs de $E(\mathbf{Q})/2E(\mathbf{Q})$. Mais à l'heure actuelle, on ne dispose pas d'algorithme général pour répondre à cette question.

La hauteur $h : E(\mathbf{Q}) \to \mathbf{R}$ construite précédemment dépend du choix de l'équation de Weierstraß. Nous allons maintenant construire une hauteur canonique sur $E(\mathbf{Q})$.

Proposition 5.15. — *Pour tout point $P \in E(\mathbf{Q})$, la suite $h(2^n P)/4^n$ converge et sa limite ne dépend pas de l'équation de Weierstraß.*

Démonstration. — En reprenant la preuve du lemme 5.13, on voit qu'il existe une constante C' telle que pour tout $P \in E(\mathbf{Q})$ on ait $h(2P) \leq 4h(P) + C'$ (c'est l'inégalité facile). Choisissons donc C telle que pour tout $P \in E(\mathbf{Q})$ on ait $|h(2P) - 4h(P)| \leq C$.

Soit $P \in E(\mathbf{Q})$. Posons $u_n = h(2^n P)/4^n$. Alors

$$|u_{n+1} - u_n| = \left| \frac{h(2^{n+1}P) - 4h(2^n P)}{4^{n+1}} \right| \leq \frac{C}{4^{n+1}} \qquad (n \geq 0).$$

Il en résulte que la série $\sum(u_{n+1} - u_n)$ converge, donc u_n converge.

Soit $(y')^2 = (x')^3 + a'x' + b'$ une autre équation de Weierstraß pour E et $h' : E(\mathbf{Q}) \to \mathbf{R}$ la hauteur associée. Les deux équations sont reliées par un changement de variables $x = u^2x' + r$ et $y = u^3y' + u^2sx' + t$ et l'examen des coefficients donne $r = s = t = 0$. Donc $x = u^2x'$ et la quantité $h(x(Q)) - h(x'(Q))$ est bornée indépendamment de $Q \in E(\mathbf{Q})$. Par suite $h - h'$ est bornée sur $E(\mathbf{Q})$, et en notant $u'_n = h'(2^n P)/4^n$, il vient $u_n - u'_n \to 0$. □

Définition 5.16. — La *hauteur de Néron-Tate* $\widehat{h} : E(\mathbf{Q}) \to \mathbf{R}$ est donnée par $\widehat{h}(P) \lim_{n\to\infty} h(2^n P)/4^n$ pour tout $P \in E(\mathbf{Q})$.

Si A est un groupe abélien, une application $q : A \to \mathbf{R}$ est une forme quadratique si elle vérifie les deux propriétés suivantes :

(1) pour tout $m \in \mathbf{Z}$ et $x \in A$, on a $q(mx) = m^2 q(x)$;

(2) l'application $(x, y) \mapsto q(x + y) - q(x) - q(y)$ est $\mathbf{Z}$-bilinéaire.

Théorème 5.17. — *La hauteur de Néron-Tate est une forme quadratique sur* $E(\mathbf{Q})$.

Démonstration. — Comme $x(-P) = x(P)$, on a $\widehat{h}(-P) = \widehat{h}(P)$ et la définition de $\widehat{h}$ donne facilement $\widehat{h}(2P) = 4\widehat{h}(P)$ pour tout $P \in E(\mathbf{Q})$.

Pour $P, Q \in E(\mathbf{Q})$, posons $\langle P, Q\rangle = \widehat{h}(P + Q) - \widehat{h}(P) - \widehat{h}(Q)$. En particulier $\langle P, P\rangle = 2\widehat{h}(P)$. Si nous montrons que $\langle \cdot, \cdot \rangle$ est bilinéaire, alors $\widehat{h}((m + 1)P) = \widehat{h}(mP) + \widehat{h}(P) + m\langle P, P\rangle$ et une récurrence immédiate donne $\widehat{h}(mP) = m^2\widehat{h}(P)$ pour $m \geq 2$, d'où la propriété (1).

Commençons par montrer que $\widehat{h}$ vérifie la loi du parallélogramme :

$$\widehat{h}(P + Q) + \widehat{h}(P - Q) = 2\widehat{h}(P) + 2\widehat{h}(Q) \qquad (P, Q \in E(\mathbf{Q})). \tag{12}$$

Posons $E : y^2 = x^3 + ax + b$ avec $a, b \in \mathbf{Z}$. Montrons qu'il existe C telle que pour tout $P, Q \in E(\mathbf{Q})$ on ait

$$h(P+Q)+h(P-Q)\leq 2h(P)+2h(Q)+C. \tag{13}$$

Pour $P=O$ ou $Q=O$, l'inégalité (13) est vraie. D'autre part, le cas $Q=\pm P$ a déjà été traité. On peut donc supposer $P=(x_1,y_1)$, $Q=(x_2,y_2)$, $P+Q=(x_3,y_3)$ et $P-Q=(x_4,y_4)$. La formule d'addition donne

$$\begin{cases} x_3=\lambda^2-x_1-x_2 \\ x_4=\mu^2-x_1-x_2 \end{cases} \qquad \text{avec} \quad \begin{cases} \lambda=\frac{y_2-y_1}{x_2-x_1} \\ \mu=\frac{-y_2-y_1}{x_2-x_1} \end{cases}$$

d'où l'on tire

$$x_3+x_4=\frac{2(x_1+x_2)(x_1x_2+a)+4b}{(x_1-x_2)^2}$$
$$x_3x_4=\frac{(x_1x_2-a)^2-4b(x_1+x_2)}{(x_1-x_2)^2}.$$

Posons $x_i=u_i/v_i$ avec $u_i,v_i\in\mathbf{Z}$ premiers entre eux. En multipliant numérateurs et dénominateurs par $v_1^2v_2^2$, on peut écrire $x_3+x_4=u/w$ et $x_3x_4=v/w$ avec $u,v,w\in\mathbf{Z}$ et

$$M:=\max(|u|,|v|,|w|)\leq C_1H(x_1)^2H(x_2)^2$$

et où C_1 ne dépend que de a et b. Par ailleurs

$$x_3+x_4=\frac{u_3v_4+u_4v_3}{v_3v_4} \qquad x_3x_4=\frac{u_3u_4}{v_3v_4}$$

et on vérifie que les entiers $u_3v_4+u_4v_3$, u_3u_4 et v_3v_4 sont premiers entre eux dans leur ensemble, donc divisent respectivement u, v et w. Enfin

$$\begin{aligned}(u_3v_4-u_4v_3)^2&=(u_3v_4+u_4v_3)^2-4u_3u_4v_3v_4\\&\leq u^2+4|vw|\leq 5M^2.\end{aligned}$$

On en déduit $u_3^2v_4^2+u_4^2v_3^2\leq 3M^2$ d'où

$$\max(|u_3|,|v_3|)\cdot\max(|u_4|,|v_4|)\leq\sqrt{3}\cdot M$$

et on obtient (13) en passant au logarithme. En passant à la hauteur de Néron-Tate, on a l'inégalité $\leq$ dans (12).

Soit $P, Q \in E(\mathbf{Q})$. Posant $P' = P + Q$ et $Q' = P - Q$, il vient

$$\begin{aligned} 2\widehat{h}(P) + 2\widehat{h}(Q) &= \frac{1}{2}\big(\widehat{h}(2P) + \widehat{h}(2Q)\big) \\ &= \frac{1}{2}\big(\widehat{h}(P' + Q') + \widehat{h}(P' - Q')\big) \\ &\leq \widehat{h}(P') + \widehat{h}(Q') \end{aligned}$$

ce qui achève de montrer (12). En particulier

$$\begin{aligned} 2\langle P, Q\rangle &= 2\widehat{h}(P + Q) - \widehat{h}(P + Q) - \widehat{h}(P - Q) \\ &= \widehat{h}(P + Q) - \widehat{h}(P - Q). \end{aligned} \tag{14}$$

Montrons enfin la bilinéarité de $\langle \cdot, \cdot \rangle$. Par symétrie, il suffit de montrer la linéarité à gauche. Posons $F(P, Q, R) = 2\langle P + Q, R\rangle - 2\langle P, R\rangle - 2\langle Q, R\rangle$. D'après (14) et la loi du parallélogramme, il vient

$$\begin{aligned} F(P, Q, R) &= \widehat{h}(P + R + Q) - \widehat{h}(P + R - Q) - \widehat{h}(P + Q) + \widehat{h}(P - Q) \\ &\quad - \widehat{h}(R + Q) + \widehat{h}(R - Q) \\ &= \frac{\widehat{h}(2P + R) + \widehat{h}(R + 2Q)}{2} - \frac{\widehat{h}(2P + R) + \widehat{h}(R - 2Q)}{2} \\ &\quad - \widehat{h}(R + Q) + \widehat{h}(R - Q) \end{aligned}$$

qui ne dépend pas de P, donc $F(P, Q, R) = F(O, Q, R) = 0$. □

Soit E une courbe elliptique sur $\mathbf{Q}$ et $r = \operatorname{rang} E(\mathbf{Q})$, de sorte que $E(\mathbf{Q})/E(\mathbf{Q})_{\text{torsion}} \cong \mathbf{Z}^r$. Notons $P_1, \ldots, P_r$ des représentants dans $E(\mathbf{Q})$ d'une $\mathbf{Z}$-base de $E(\mathbf{Q})/E(\mathbf{Q})_{\text{torsion}}$.

Définition 5.18. — Le *régulateur* de E est $R_E = \det(\langle P_i, P_j\rangle)_{1 \leq i,j \leq r}$.

Proposition 5.19. — *Le régulateur ne dépend pas du choix des P_i et on a $R_E > 0$.*

Démonstration. — Par convention, on a $R_E = 1$ si $r = 0$. On peut donc dorénavant supposer $r \geq 1$.

Si $P \in E(\mathbf{Q})_{\text{torsion}}$ alors il existe m tel que $mP = O$, ce qui entraîne $\langle P, Q\rangle = \frac{1}{m}\langle mP, Q\rangle = 0$ pour tout $Q \in E(\mathbf{Q})$. Par suite $\langle \cdot, \cdot \rangle$ se factorise

par $E(\mathbf{Q})/E(\mathbf{Q})_{\text{torsion}}$ et R_E dépend au plus du choix de la $\mathbf{Z}$-base. Si $(P'_1, \dots, P'_r)$ est une autre base de $E(\mathbf{Q})/E(\mathbf{Q})_{\text{torsion}}$, alors R_E est multiplié par le carré du déterminant d'une matrice de $\mathrm{GL}_r(\mathbf{Z})$, donc est inchangé.

Considérons la matrice symétrique $M = (\langle P_i, P_j \rangle) \in \mathcal{M}_r(\mathbf{R})$. Puisque $\widehat{h} \geq 0$ on a $q(x) = {}^t xMx \geq 0$ pour tout $x \in \mathbf{Z}^r$, donc pour tout $x \in \mathbf{Q}^r$ et par continuité, q est positive. Il reste à montrer que M est inversible. Soit C telle que pour tout $P \in E(\mathbf{Q})$ on ait $h(P) \leq h(2P)/4 + C$. Par une récurrence immédiate il vient $h(P) \leq h(2^n P)/4^n + 4C/3$ et en passant à la limite $h(P) \leq \widehat{h}(P) + 4C/3$ pour tout P. Si maintenant $\widehat{h}(P) = 0$ alors $\widehat{h}(mP) = 0$ pour tout m, donc la suite $(h(mP))$ est bornée et par le lemme 5.11, on en déduit que P est de torsion. Par suite $q(x) > 0$ si $x \in \mathbf{Z}^r$, $x \neq 0$. De plus, comme $h - \widehat{h}$ est majorée, l'ensemble $\{P \in E(\mathbf{Q}); \widehat{h}(P) \leq C'\}$ est fini pour tout C', et il est licite de poser $\lambda = \min\{q(x); x \in \mathbf{Z}^r, x \neq 0\}$. Supposons par l'absurde que q n'est pas définie positive. Alors la partie convexe symétrique $C = \{x \in \mathbf{R}^r; q(x) \leq \lambda/2\}$ est de volume infini (écrire q comme somme de carrés). Par le théorème de Minkowski, C contient un point non nul de $\mathbf{Z}^r$, ce qui contredit la définition de λ. Ainsi $R_E > 0$. □

Nous introduisons maintenant la notion d'équation de Weierstraß minimale. Nous avons vu que pour toute courbe elliptique E sur $\mathbf{Q}$ et tout nombre premier p, la courbe E possède une équation minimale en p.

Proposition 5.20. — *Toute courbe elliptique sur* $\mathbf{Q}$ *possède une équation de Weierstraß à coefficients dans* $\mathbf{Z}$ *qui est minimale en tout nombre premier* p.

Remarque 5.21. — Une telle équation est dite *globalement minimale* ; son discriminant est le *discriminant minimal* de E.

Démonstration. — Prenons une équation de Weierstraß pour E à coefficients $a_i \in \mathbf{Z}$, de discriminant Δ. Soit S l'ensemble (fini) des nombres premiers p tels que l'équation n'est pas minimale en p. Pour tout $p \in S$, notons $a_{i,p}$ les coefficients d'une équation minimale en p. Par densité de $\mathbf{Q}$ dans $\mathbf{Q}_p$, on peut prendre $a_{i,p} \in \mathbf{Q}$. Soit (r_p, s_p, t_p, u_p) un changement de variables vers cette équation minimale. Par la même démonstration

que pour la proposition 4.10, on a $v_p(r_p), v_p(s_p), v_p(t_p), v_p(u_p) \geq 0$. Soit $u = \prod_{p \in S} p^{v_p(u_p)}$. Par le théorème des restes chinois, il existe $r, s, t \in \mathbf{Z}$ tels que

$$v_p(r - r_p), v_p(s - s_p), v_p(t - t_p) > \max_i v_p(u_p^i a_{i,p}) \qquad (p \in S).$$

On vérifie alors que le changement de variables (r, s, t, u) conduit à une équation globalement minimale pour E. □

Pour terminer, donnons l'énoncé du théorème de Siegel, concernant les points entiers des courbes elliptiques.

***Théorème 5.22* (Siegel).** — *Soit E une courbe elliptique sur $\mathbf{Q}$. Pour toute $f \in \mathbf{Q}(E)$ non constante, l'ensemble $\{P \in E(\mathbf{Q}); f(P) \in \mathbf{Z}\}$ est fini. En particulier, la courbe E ne possède qu'un nombre fini de points à coordonnées entières.*

Exercices. — **5.1.** Soit E une courbe elliptique sur $\mathbf{Q}$. Soit $m \geq 1$ et K le corps engendré par les coordonnées des points de m-torsion de E.

(a) Montrer que l'action de $\mathrm{Gal}(K/\mathbf{Q})$ sur $E[m]$ induit un morphisme injectif de groupes $\rho_m : \mathrm{Gal}(K/\mathbf{Q}) \to \mathrm{Aut}(E[m])$.

(b) Lorsque $m = 2$, en déduire $[K : \mathbf{Q}] \leq 6$; déterminer les groupes de Galois possibles et montrer que chaque cas se produit effectivement.

(c) On suppose que E a bonne réduction en p premier ne divisant pas m. Montrer que $K/\mathbf{Q}$ est non ramifiée en p.

5.2. Soit $\psi : E \to E'$ une isogénie entre deux courbes elliptiques définies sur $\mathbf{Q}$. On suppose que ψ est définie sur $\mathbf{Q}$. Montrer que les rangs de $E(\mathbf{Q})$ et de $E'(\mathbf{Q})$ sont égaux.

5.3. (cf. démonstration du lemme 5.13) Soit $a, b \in \mathbf{Z}$ tels que $\Delta = 4a^3 + 27b^2 \neq 0$. On pose $F = X^4 - 2aX^2 - 8bX + a^2$ et $G = X^3 + aX + b$. Déterminer des polynômes F_1 et G_1 (resp. F_2 et G_2) dans $\mathbf{Z}[X]$, de degrés 2 et 3 (resp. 3 et ≤ 3) tels que $F_1F + G_1G = \Delta$ (resp. $F_2F + G_2G = \Delta \cdot X^7$).

5.4. Soit E une courbe elliptique sur $\mathbf{Q}$.

(a) Montrer que $h - 2\widehat{h}$ est bornée sur $E(\mathbf{Q})$.

(b) Soit $\widehat{h}'$ une fonction $E(\mathbf{Q}) \to \mathbf{R}$ telle que $h - 2\widehat{h}'$ est bornée et $\widehat{h}'(2P) = 4\widehat{h}'(P)$ pour tout $P \in E(\mathbf{Q})$. Montrer $\widehat{h} = \widehat{h}'$.

5.5. Soit E une courbe elliptique sur $\mathbf{Q}$ et $Q_1, \ldots, Q_s$ un système de représentants de $E(\mathbf{Q})/2E(\mathbf{Q})$ dans $E(\mathbf{Q})$. Posons $t = \max \widehat{h}(Q_i)$. Montrer que $E(\mathbf{Q})$ est engendré par $\{P \in E(\mathbf{Q}); \widehat{h}(P) \leq t\}$.

5.6. Dans quelle mesure l'équation de Weierstraß minimale globale d'une courbe elliptique sur $\mathbf{Q}$ est-elle unique ?

6. La conjecture de Birch et Swinnerton-Dyer

Le rang du groupe des points rationnels d'une courbe elliptique est un invariant difficile à déterminer en général. Il est plus facile de calculer le nombre de solutions de l'équation définissant la courbe elliptique modulo un nombre premier. La conjecture de Birch et Swinnerton-Dyer fournit une relation entre ces deux problèmes. Pour énoncer la conjecture, nous avons besoin de définir la fonction L associée à une courbe elliptique.

Soit E une courbe elliptique définie sur $\mathbf{Q}$, et p un nombre premier. La réduction $\widetilde{E}$ de E modulo p est une courbe projective définie sur $\mathbf{F}_p$. Posons

$$\operatorname{card} \widetilde{E}(\mathbf{F}_p) = p + 1 - a_p \qquad (a_p \in \mathbf{Z}).$$

Définition 6.1. — Pour $s \in \mathbf{C}$, on pose

$$L_p(E, s) = \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \qquad \text{si } E \text{ a bonne réduction en } p,$$

$$L_p(E, s) = \frac{1}{1 - a_p p^{-s}} \qquad \text{sinon.}$$

Si E a bonne réduction en p, alors $\widetilde{E}$ est une courbe elliptique et le théorème de Hasse donne l'estimation $|a_p| \leq 2\sqrt{p}$.

Si E a mauvaise réduction en p, le point singulier de $\widetilde{E}$ est toujours défini sur $\mathbf{F}_p$, ce qui fait que $\operatorname{card} \widetilde{E}(\mathbf{F}_p) = 1 + \operatorname{card} \widetilde{E}_{\mathrm{ns}}(\mathbf{F}_p)$. D'autre part, on a vu que $\widetilde{E}_{\mathrm{ns}}$ est isomorphe soit au groupe multiplicatif $\overline{\mathbf{F}_p}^*$, soit au groupe additif $\overline{\mathbf{F}_p}$. On parle respectivement de réduction multiplicative et additive.

Dans le cas multiplicatif, on peut montrer que $\widetilde{E}_{\mathrm{ns}}(\mathbf{F}_p)$ est isomorphe à $\mathbf{F}_p^*$ ou au groupe des éléments de norme 1 de $\mathbf{F}_{p^2}^*$. On a alors $\operatorname{card} \widetilde{E}_{\mathrm{ns}}(\mathbf{F}_p) =$

$p \pm 1$, ce qui conduit à $a_p = \pm 1$. Dans le cas additif, on a $\widetilde{E}_{\mathrm{ns}}(\mathbf{F}_p) \cong \mathbf{F}_p$ et donc $a_p = 0$.

Dans tous les cas, $L_p(E, s)$ est défini (au moins) pour $\Re(s) > \frac{1}{2}$.

Définition 6.2. — La *fonction L de Hasse-Weil de E* est donnée par

$$L(E, s) = \prod_{p \text{ premier}} L_p(E, s).$$

Ce produit eulérien converge pour $\Re(s) > \frac{3}{2}$ d'après les bornes de Hasse, et comme il y a convergence sur tout compact, $L(E, s)$ est une fonction holomorphe sur ce demi-plan.

Théorème **(Breuil, Conrad, Diamond, Taylor, Wiles)**
La fonction $L(E, s)$ se prolonge en une fonction holomorphe sur $\mathbf{C}$.

Hasse avait conjecturé le prolongement méromorphe de $L(E, s)$. Le théorème énoncé ci-dessus est conséquence d'un résultat plus précis : toute courbe elliptique définie sur $\mathbf{Q}$ est "modulaire". Avant d'expliquer ce terme, nous allons définir le conducteur de la courbe elliptique.

Le conducteur de E est l'entier $N = N_E$ donné par

$$N = \prod_{p \text{ premier}} p^{f_p}$$

où $f_p = \varepsilon_p + \delta_p$ et les entiers ε_p et δ_p sont définis comme suit. L'entier ε_p, qui mesure la mauvaise réduction de E, est donné par

$$\varepsilon_p = \begin{cases} 0 & \text{si } E \text{ a bonne réduction en } p\,; \\ 1 & \text{si } E \text{ a réduction multiplicative en } p\,; \\ 2 & \text{si } E \text{ a réduction additive en } p. \end{cases}$$

L'entier δ_p mesure la "ramification sauvage" des points de torsion de E. Soit ℓ un nombre premier $\neq p$, et K le corps engendré par les coordonnées des points de $E[\ell]$. L'extension $K/\mathbf{Q}$ est finie galoisienne et $\mathrm{Gal}(K/\mathbf{Q})$ agit linéairement et fidèlement sur $E[\ell]$, qui est un $\mathbf{Z}/\ell\mathbf{Z}$-espace vectoriel de dimension 2. Soit $\mathfrak{p}$ un idéal premier de K au-dessus de p. Le groupe $G = \mathrm{Gal}(K_{\mathfrak{p}}/\mathbf{Q}_p)$ s'identifie au sous-groupe de décomposition de $\mathfrak{p}$ dans $\mathrm{Gal}(K/\mathbf{Q})$. Rappelons que G est muni de la filtration de ramification

(finie) $G \supset G_0 \supset G_1 \supset \cdots$. Si π est une uniformisante de K, on a $G_u = \{\sigma \in G; v_K(\sigma\pi - \pi) \geq u+1\}$ où la valuation est normalisée par $v_K(\pi) = 1$. En particulier, G_0 est le sous-groupe d'inertie de G. On pose alors

$$\delta_p = \sum_{u \geq 1} \frac{|G_u|}{|G_0|} \cdot \dim_{\mathbf{Z}/\ell\mathbf{Z}} \frac{E[\ell]}{E[\ell]^{G_u}}.$$

Ogg a donné une formule géométrique pour δ_p, qui montre en particulier que δ_p est entier et ne dépend pas de ℓ (ce qui n'est pas évident avec cette définition). Il est à noter que $\delta_p = 0$ si et seulement si $G_1 = \{1\}$, *i. e.* l'extension $K/\mathbf{Q}$ est modérément ramifiée en $\mathfrak{p}$. Si E a bonne réduction en p, on a vu (lemme 5.7) que $K/\mathbf{Q}$ est non ramifiée en $\mathfrak{p}$, donc $G_0 = \{1\}$ et $\delta_p = 0$. Dans le cas de réduction multiplicative, on a aussi $\delta_p = 0$. Dans le cas de réduction additive on a $\delta_p = 0$ si $p \neq 2, 3$.

En développant $L_p(E,s)$ comme série formelle en p^{-s}, on a $L_p(E,s) = \sum_{k\geq 0} a_{p^k} p^{-ks}$ où $a_1 = 1$ et $a_{p^k} \in \mathbf{Z}$ s'exprime en termes de a_p. Le développement du produit eulérien montre que la fonction L de E est une série de Dirichlet $L(E,s) = \sum_{n\geq 1} a_n/n^s$, qui converge au moins pour $\Re(s) > \frac{3}{2}$. De plus $a_n \in \mathbf{Z}$ et la fonction $n \mapsto a_n$ est multiplicative : si m et n sont premiers entre eux alors $a_{mn} = a_m a_n$. On peut ainsi calculer a_n pour tout entier $n \geq 1$.

Soit $\mathcal{H} = \{z \in \mathbf{C}; \Im(z) > 0\}$ le demi-plan de Poincaré. Le groupe $\mathrm{SL}_2(\mathbf{Z})$ agit sur $\mathcal{H}$ par la règle

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

Pour tout $z \in \mathcal{H}$, on pose $q = e^{2i\pi z}$ et $f_E(z) = \sum_{n\geq 1} a_n q^n$. Puisque $|q| = e^{-2\pi\Im(z)} < 1$, cette série de fonctions converge normalement sur $\{z \in \mathcal{H}; \Im(z) \geq y_0 > 0\}$ et définit donc une fonction holomorphe sur $\mathcal{H}$. Notons $\Gamma_0(N)$ le sous-groupe de $\mathrm{SL}_2(\mathbf{Z})$ formé des matrices vérifiant

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N}.$$

***Théorème* (Breuil, Conrad, Diamond, Taylor, Wiles)**
La fonction f_E vérifie les propriétés de modularité

$$f_E\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f_E(z) \qquad \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N), z \in \mathcal{H}\right) \tag{15}$$

$$f_E\left(-\frac{1}{Nz}\right) = wNz^2 f_E(z) \qquad (w = \pm 1, z \in \mathcal{H}). \tag{16}$$

La fonction $L(E,s)$ est reliée à f_E par le calcul fondamental suivant

$$\begin{aligned}\int_0^\infty f_E(iy) y^{s-1} dy &= \sum_{n\geq 1} a_n \int_0^\infty e^{-2\pi n y} y^{s-1} dy \\ &= \sum_{n\geq 1} a_n (2\pi n)^{-s} \int_0^\infty e^{-u} u^{s-1} du \\ &= (2\pi)^{-s}\Gamma(s) L(E,s).\end{aligned}$$

En découpant l'intégrale ci-dessus et en effectuant le changement de variables $y' = 1/(Ny)$, la propriété (16) entraîne

$$(2\pi)^{-s}\Gamma(s)L(E,s) = \int_{1/\sqrt{N}}^\infty f_E(iy) \cdot (y^{s-1} - wN^{1-s}y^{1-s}) dy. \tag{17}$$

Puisque $f_E(iy) = O_{y\to+\infty}(e^{-2\pi y})$, on en déduit que $(2\pi)^{-s}\Gamma(s)L(E,s)$, et donc $L(E,s)$, se prolonge en une fonction holomorphe sur $\mathbf{C}$. Par ailleurs, en posant $\Lambda(E,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$, la formule (17) entraîne l'équation fonctionnelle

$$\Lambda(E,s) = -w\Lambda(E,2-s) \qquad (s \in \mathbf{C}).$$

À titre d'exercice, on pourra exprimer $L(E,1)$ en termes de f_E.

Nous allons maintenant définir les différents ingrédients intervenant dans la conjecture de Birch et Swinnerton-Dyer. D'après la proposition 5.20, E possède une équation de Weierstraß

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in \mathbf{Z})$$

qui est globalement minimale, c'est-à-dire minimale en tout nombre premier p.

Proposition 6.3. — *La forme différentielle invariante* $\omega_E = dx/(2y + a_1x + a_3)$ *est bien définie au signe près.*

Démonstration. — On montre que deux équations globalement minimales sont reliées par un changement de variables $x = x'$ et $y = \pm y' + sx' + t$ avec $s, t \in \mathbf{Z}$, et les deux formes différentielles associées ω et ω' sont égales au signe près. □

Le groupe $E(\mathbf{C})$ est isomorphe au tore complexe $\mathbf{C}/\Lambda_E$, où Λ_E est le *réseau des périodes* de ω_E, c'est-à-dire l'ensemble des $\int_\gamma \omega_E$, où γ parcourt le groupe fondamental de $E(\mathbf{C})$. Comme E et ω_E sont définies sur $\mathbf{Q}$, donc sur $\mathbf{R}$, le réseau Λ_E est invariant par la conjugaison complexe. Le groupe $E(\mathbf{R})$ s'identifie alors aux points fixes de la conjugaison complexe $c : [z] \mapsto [\overline{z}]$ sur $\mathbf{C}/\Lambda_E$. Il y a deux cas :

(1) On a $\Lambda_E = \Omega_E^+ \cdot \mathbf{Z} + i\Omega_E^- \cdot \mathbf{Z}$ avec $\Omega_E^+, \Omega_E^- > 0$. Dans ce cas $E(\mathbf{R})$ possède deux composantes connexes et $|\int_{E(\mathbf{R})} \omega_E| = 2\Omega_E^+$.

(2) On a $\Lambda_E = \Omega_E^+ \cdot \mathbf{Z} + \frac{1}{2}(\Omega_E^+ + i\Omega_E^-) \cdot \mathbf{Z}$ avec $\Omega_E^+, \Omega_E^- > 0$. Dans ce cas $E(\mathbf{R})$ est connexe et $|\int_{E(\mathbf{R})} \omega_E| = \Omega_E^+$.

Le groupe de Galois $G_\mathbf{Q} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ agit linéairement sur $E = E(\overline{\mathbf{Q}})$. Nous allons définir le groupe de cohomologie galoisienne $H^1(G_\mathbf{Q}, E)$ [**3**, Appendix B].

Définition 6.4. — Un $G_\mathbf{Q}$-module est un groupe abélien M muni d'une action linéaire de $G_\mathbf{Q}$ et vérifiant la propriété suivante : pour tout $m \in M$, il existe une extension finie $K/\mathbf{Q}$ telle que G_K agit trivialement sur m (cela revient à dire que l'appplication $\sigma \mapsto \sigma m$ est continue pour la topologie profinie sur $G_\mathbf{Q}$ et la topologie discrète sur M).

Par exemple, $\overline{\mathbf{Q}}$, $\overline{\mathbf{Q}}^*$ et E sont des $G_\mathbf{Q}$-modules.

Définition 6.5. — Soit M un $G_\mathbf{Q}$-module. Le groupe des 1-cocyles $Z^1(G_\mathbf{Q}, M)$ est l'ensemble des applications $f : G_\mathbf{Q} \to M$ qui sont continues (c'est-à-dire localement constantes : pour tout $\sigma_0 \in G_\mathbf{Q}$, il existe $K/\mathbf{Q}$ finie telle que f est constante sur $\sigma_0 G_K$) et qui vérifient

$$f(\sigma\tau) = \sigma f(\tau) + f(\sigma) \qquad (\sigma, \tau \in G_\mathbf{Q}).$$

Le groupe des 1-cobords $B^1(G_{\mathbf{Q}}, M)$ est l'ensemble des applications $f : G_{\mathbf{Q}} \to M$ de la forme $f(\sigma) = \sigma m - m$ pour $m \in M$.

On vérifie que $B^1(G_{\mathbf{Q}}, M)$ est un sous-groupe de $Z^1(G_{\mathbf{Q}}, M)$.

Définition 6.6. — On pose $H^1(G_{\mathbf{Q}}, M) = Z^1(G_{\mathbf{Q}}, M)/B^1(G_{\mathbf{Q}}, M)$.

Si p est un nombre premier, on peut considérer E comme une courbe elliptique sur $\mathbf{Q}_p$ et définir comme ci-dessus le groupe de cohomologie $H^1(G_{\mathbf{Q}_p}, E(\overline{\mathbf{Q}_p}))$. De même pour $G_{\mathbf{R}} = \mathrm{Gal}(\mathbf{C}/\mathbf{R})$, on a le groupe $H^1(G_{\mathbf{R}}, E(\mathbf{C}))$.

Choisissons un plongement $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}_p}$. Cela permet d'identifier le groupe de Galois $G_{\mathbf{Q}_p} = \mathrm{Gal}(\overline{\mathbf{Q}_p}/\mathbf{Q}_p)$ à un sous-groupe (de décomposition) de $G_{\mathbf{Q}}$; il est bien défini à conjugaison près dans $G_{\mathbf{Q}}$. De même, le choix d'un plongement $\overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$ induit $G_{\mathbf{R}} \subset G_{\mathbf{Q}}$.

Posons $\mathbf{Q}_\infty = \mathbf{R}$ (donc $\overline{\mathbf{Q}_\infty} = \mathbf{C}$). Dans ce qui suit, on traitera uniformément le cas où v est un nombre premier ou ∞. Posons $E_v = E(\overline{\mathbf{Q}_v})$. Soit $f : G_{\mathbf{Q}} \to E(\overline{\mathbf{Q}})$ un 1-cocycle. Les inclusions $G_{\mathbf{Q}_v} \subset G_{\mathbf{Q}}$ et $E \hookrightarrow E_v$ induisent un 1-cocyle $f_v : G_{\mathbf{Q}_v} \to E_v$. L'application $f \mapsto f_v$ induit un morphisme de groupes $H^1(G_{\mathbf{Q}}, E) \to H^1(G_{\mathbf{Q}_v}, E_v)$.

Définition 6.7. — Le *groupe de Tate-Shafarevich* de E, noté $Ш(E)$, est le noyau de l'application

$$H^1(G_{\mathbf{Q}}, E) \to \prod_v H^1(G_{\mathbf{Q}_v}, E_v)$$

où v parcourt les nombres premiers et ∞.

Enfin, pour p premier, on note c_p l'indice de $E_0(\mathbf{Q}_p)$ dans $E(\mathbf{Q}_p)$ (cf. proposition 4.16). On sait que $c_p = 1$ si E a bonne réduction en p.

***Conjecture* (Birch et Swinnerton-Dyer)**. — (1) L'ordre d'annulation de $L(E, s)$ en $s = 1$ est égal au rang r du groupe $E(\mathbf{Q})$.

(2) Le groupe $Ш(E)$ est fini, et l'on a

$$\lim_{s \to 1} \frac{L(E, s)}{(s-1)^r} = \frac{Ш(E) \prod_p c_p}{|E(\mathbf{Q})_{\mathrm{torsion}}|^2} \cdot \left| \int_{E(\mathbf{R})} \omega_E \right| \cdot R_E. \tag{18}$$

Il y a là un phénomène remarquable : le comportement local de E, à savoir le nombre de solutions de l'équation modulo chaque nombre premier p, détermine le rang de E, qui est un invariant global.

Remarque 6.8. — La conjecture prédit en particulier que $E(\mathbf{Q})$ est infini si et seulement si $L(E,1)=0$. On peut faire le raisonnement heuristique suivant pour expliquer cette équivalence : si $E(\mathbf{Q})$ est infini, alors en réduisant modulo p, on espère obtenir "beaucoup" de solutions dans $\mathbf{F}_p$, c'est-à-dire que a_p est "proche" de $-2\sqrt{p}$, et en considérant le produit eulérien, on s'attend à $L(E,1)=0$. Historiquement, Birch et Swinnerton-Dyer ont étudié numériquement le produit $\prod_{p\leq x}\frac{\operatorname{card}\widetilde{E}(\mathbf{F}_p)}{p}$, et ont constaté qu'il croît comme $(\log x)^r$.

La conjecture de Birch et Swinnerton-Dyer se généralise

(a) aux courbes elliptiques définies sur les corps de nombres et sur les corps de fonctions (extensions finies de $\mathbf{F}_p(T)$) ;

(b) aux variétés abéliennes (l'analogue des courbes elliptiques en dimension $d\geq 1$; le facteur en p de la fonction L est cette fois un polynôme de degré $2d$ en p^{-s}) ;

(c) aux fonctions L p-adiques (conjecture de Mazur-Tate-Teitelbaum).

Donnons un aperçu des résultats connus. La conjecture est stable par isogénie : si deux courbes elliptiques E et E' sont reliées par une isogénie $E\to E'$ non nulle définie sur $\mathbf{Q}$, alors la conjecture est vraie pour E si et seulement si elle est vraie pour E' (voir à ce sujet les exercices 5.2 et 6.1). En revanche, dans le membre de droite de (18), aucun des facteurs n'est nécessairement invariant par isogénie.

Concernant le groupe de Tate-Shafarevich, on sait que :

(1) le groupe $Ш(E)$ est de torsion ;

(2) pour tout $n\geq 1$, le groupe de n-torsion $Ш(E)[n]$ est fini ;

(3) si ℓ est premier, alors $Ш(E)[\ell^\infty]:=\cup_{n\geq 1}Ш[\ell^n]\cong F\times(\mathbf{Q}_\ell/\mathbf{Z}_\ell)^r$ avec F fini et $r\geq 0$ (on dit que la ℓ-partie de $Ш(E)$ est de corang fini, où le corang est défini par $\operatorname{rg}_{\mathbf{Z}_\ell}\operatorname{Hom}_{\mathbf{Z}}(\cdot,\mathbf{Q}_\ell/\mathbf{Z}_\ell)$) ;

(4) si $Ш(E)$ est fini, son ordre est un carré parfait (l'analogue pour les variétés abéliennes est faux).

Il est usuel de définir le *rang analytique* de E par $r_E^{\mathrm{an}} = \mathrm{ord}_{s=1} L(E,s)$. Kolyvagin a montré, en utilisant la formule de Gross-Zagier et des techniques cohomologiques, que si E est une courbe elliptique sur $\mathbf{Q}$ vérifiant $r_E^{\mathrm{an}} \leq 1$, alors $r_E^{\mathrm{an}} = \mathrm{rg}\, E(\mathbf{Q})$, $Ш(E)$ est fini et (18) est vraie à un facteur rationnel non nul près. Il n'existe à l'heure actuelle aucun résultat de ce type lorsque $r_E^{\mathrm{an}} \geq 2$. Cependant, dans la direction p-adique, Kato a montré que le rang de $E(\mathbf{Q})$ est toujours inférieur ou égal à l'ordre d'annulation de la fonction L p-adique associée à E ; on ne dispose pas d'équivalent de ce résultat dans la situation complexe.

Exercices. — **6.1.** Soit E une courbe elliptique sur $\mathbf{Q}$ ayant bonne réduction en p, et $\widetilde{E}$ la réduction de E modulo p. Soit ℓ premier $\neq p$ et K le corps engendré par les coordonnées des points de $E[\ell]$. On sait (exercice 5.1) que $K/\mathbf{Q}$ est non ramifiée en p ; on dispose donc du Frobenius $(\mathfrak{p}, K/\mathbf{Q})$ pour tout idéal premier $\mathfrak{p} \subset \mathcal{O}_K$ au-dessus de p.

(a) En réduisant modulo $\mathfrak{p}$, définir une bijection $E[\ell] \to \widetilde{E}[\ell]$.

(b) En considérant le Frobenius de $\widetilde{E}$, montrer que le polynôme caractéristique de $(\mathfrak{p}, K/\mathbf{Q})$ sur $E[\ell] \cong (\mathbf{Z}/\ell\mathbf{Z})^2$ est congru $\pmod{\ell}$ à $T^2 - a_p T + p$.

(c) Soit $\psi : E \to E'$ une isogénie non nulle définie sur $\mathbf{Q}$. Déduire des questions précédentes que $\mathrm{ord}_{s=1} L(E,s) = \mathrm{ord}_{s=1} L(E',s)$.

6.2. Montrer que la forme différentielle $f_E(z)dz$ sur $\mathcal{H}$ est invariante sous l'action de $\Gamma_0(N)$. Comment se comporte-t-elle vis-à-vis de l'involution $z \mapsto -1/Nz$ de $\mathcal{H}$?

6.3. Montrer que $L(E,1) = 2\pi(1-w)\int_{1/\sqrt{N}}^{\infty} f_E(iy)dy$ et en déduire une expression de $L(E,1)$ comme somme d'une série convergente.

6.4. Pour tout entier $k \geq 0$, montrer que $L(E,s)$ a un zéro simple en $s = -k$ et exprimer $L'(E,-k)$ en termes de $L(E,k+2)$.

6.5. Soit $E : y^2 = x^3 + ax + b$ une courbe elliptique avec $a, b \in \mathbf{Q}$. Montrer que $E(\mathbf{R})$ est connexe si et seulement si $4a^3 + 27b^2 > 0$.

6.6. Que vaut $H^1(G_{\mathbf{R}}, \mathbf{C})$? $H^1(G_{\mathbf{R}}, \mathbf{C}^*)$? Si E est une courbe elliptique sur $\mathbf{Q}$, déterminer $H^1(G_{\mathbf{R}}, E(\mathbf{C}))$ suivant le nombre de composantes connexes de $E(\mathbf{R})$.

Appendice : Riemann-Roch et Riemann-Hurwitz

Nous démontrons le théorème de Riemann-Roch en suivant l'approche de Weil, reprise par Serre [**2**]. On commence par définir le résidu d'une forme différentielle algébrique. On montre ensuite une formule des résidus (théorème 6.9), et un cas particulier d'un théorème de dualité de Serre.

Soit donc C une courbe projective plane lisse de genre g. Soit t une uniformisante en $P \in C$. Au cours de la démonstration du lemme 2.42, nous avons plongé $\overline{k}(C)$ dans le corps des séries de Laurent $\overline{k}((T))$ de telle sorte que t s'envoie sur T. Soit $\omega = f dt \in \Omega^1(\overline{k}(C))$. Le *résidu* de ω en P, noté $\mathrm{Res}_P(\omega)$, est le coefficient de T^{-1} dans le développement de f en série de Laurent. Montrons que le résidu est indépendant du choix de t. Si ω est régulière en P, c'est vrai car le résidu est alors nul. Par linéarité en ω, il suffit donc de traiter le cas $f = t^{-n}$ avec $n \geq 1$. Soit t' une autre uniformisante en P. Quitte à multiplier t' par un scalaire non nul (cela ne change pas le résidu), on peut supposer $t = t' + a_2 t'^2 + \cdots$. Si $n = 1$, on a

$$\omega = \frac{dt}{t} = \frac{dt'}{t'} \cdot \frac{1 + 2a_2 t' + \cdots}{1 + a_2 t' + \cdots}$$

donc le résidu vaut 1 dans les deux cas. Supposons maintenant $n \geq 2$. Si $\mathrm{car}(\overline{k}) = 0$, on a $\omega = d(t^{1-n}/(1-n)) = h dt'$ où h est la dérivée d'une série de Laurent en T', donc ne contient pas de terme en $(T')^{-1}$: le résidu est nul dans les deux cas. En général, on peut écrire

$$\omega = \frac{dt}{t^n} = \frac{dt'}{t'^n} \cdot \frac{1 + 2a_2 t' + \cdots}{1 + n a_2 t' + \cdots} = \left(\frac{1}{t'^n} + \cdots + \frac{F(a_2, \ldots)}{t'} + \cdots \right) \cdot dt'$$

où $F(a_2, \ldots)$ est un polynôme universel à coefficients entiers en un nombre fini de a_i. Nous avons vu que ce polynôme s'annule lorsque les a_i parcourent un corps algébriquement clos de caractéristique 0 (par exemple $\mathbf{C}$). Ainsi $F = 0$, et le résidu de ω est nul dans les deux cas.

Théorème 6.9. — *Pour toute forme différentielle rationnelle ω sur C, on a $\sum_{P \in C} \mathrm{Res}_P(\omega) = 0$.*

Dans le cas où C est un tore complexe $\mathbf{C}/\Lambda$ et $\omega = f(z)dz$ avec f une fonction elliptique, ce théorème n'est autre que la proposition 1.3(1).

Démonstration. — Supposons d'abord que C est la droite projective $\mathbf{P}^1$. On a $\overline{k}(C) = \overline{k}(t)$ où t est la coordonnée naturelle de $\mathbf{A}^1$. Soit $\omega = f dt \in \Omega^1(\overline{k}(C))$ avec $f \in \overline{k}(t)$. Décomposons f en éléments simples : $f = f_\infty + \sum_{a\in\overline{k}} \sum_{i\geq 1} \lambda_{a,i}/(t-a)^i$ avec $f_\infty \in \overline{k}[t]$, et où un nombre fini de $\lambda_{a,i}$ sont non nuls. Le résidu de ω en a vaut $\lambda_{a,1}$. D'autre part, à l'infini on peut prendre $u = 1/t$ comme uniformisante. Alors $dt = -du/u^2$ et

$$\omega = \Big(-u^{-2} f_\infty(1/u) - \sum_{a\in\overline{k}} \sum_{i\geq 1} \lambda_{a,i} u^{i-2}(1-au)^{-i}\Big) \cdot du$$

d'où l'on voit que le résidu de ω à l'infini est $-\sum_{a\in\overline{k}} \lambda_{a,1}$. Ainsi la somme des résidus de ω est nulle.

Dans le cas général, on choisit une fonction rationnelle $t \in \overline{k}(C)$ telle $L = \overline{k}(C)$ soit une extension finie séparable de $K = \overline{k}(t)$ (on peut prendre par exemple une uniformisante en un point lisse de C, cf. démonstration de la proposition 2.40). On peut penser à t comme une application de C dans $\mathbf{P}^1$, avec $t(P) \in \mathbf{A}^1$ si et seulement si t est régulière en P, et $t(P) = \infty$ sinon. D'après le cas de $\mathbf{P}^1$, il est suffisant de montrer

$$\sum_{t(P)=Q} \mathrm{Res}_P(f dt) = \mathrm{Res}_Q(\mathrm{Tr}_{L/K}(f) dt) \qquad (Q \in \mathbf{P}^1). \tag{19}$$

Quitte à remplacer t par $1/t$, puis t par $t-a$, on est ramenés au cas où $Q \in \mathbf{A}^1$, puis à celui où $Q = 0$. On est alors dans la situation de la démonstration du théorème 2.35 : si B désigne la fermeture intégrale de $A = \overline{k}[t]$ dans L, les points $P_1, \ldots, P_r$ où t s'annule correspondent bijectivement aux idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ de B au-dessus de (t). Rappelons qu'en notant $tB = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, on a $\mathrm{ord}_{P_i}(t) = e_i$. Soit t_i une uniformisante en P_i. On a un diagramme commutatif

$$\begin{array}{ccc} L & \xrightarrow{\alpha_i} & \overline{k}((T_i)) \\ \uparrow & & \uparrow \\ K & \longrightarrow & \overline{k}((T)) \end{array}$$

où la flèche horizontale en haut est le développement de Laurent en t_i, celle en bas envoie t sur T, et celle à droite envoie T sur $\alpha_i(t)$, ce qui

est licite car $\alpha_i(t) \in T_i^{e_i}\overline{k}[[T_i]]$. On vérifie que l'extension $\overline{k}((T_i))/\overline{k}((T))$ est de degré e_i : une base en est donnée par $1, T_i, \ldots, T_i^{e_i-1}$. La valuation naturelle sur $\overline{k}((T_i))$ induit via α_i la valuation $\mathfrak{p}_i$-adique sur L, ce qui identifie $\overline{k}((T_i))$ au complété de L pour la valuation $\mathfrak{p}_i$-adique.

Supposons que f engendre L/K. Soit μ le polynôme minimal de f sur K. On a $t_i \in K[f]$ donc $\alpha_i(f)$ engendre $\overline{k}((T_i))/\overline{k}((T))$; soit μ_i son polynôme minimal, de degré e_i. Si $\mu_i = \mu_j$, on a un isomorphisme $\phi : \overline{k}((T_i)) \to \overline{k}((T_j))$ qui fixe $\overline{k}((T))$ et envoie $\alpha_i(f)$ sur $\alpha_j(f)$, d'où $\phi \circ \alpha_i = \alpha_j$. Comme ϕ doit envoyer uniformisante sur uniformisante, les valuations $\mathfrak{p}_i$- et $\mathfrak{p}_j$-adique sur L coïncident, d'où $i = j$. Ainsi μ est divisible par le produit des μ_i, et l'égalité des degrés entraîne $\mu = \prod_{i=1}^r \mu_i$. En considérant le terme de degré $\deg(\mu) - 1$, il vient

$$\mathrm{Tr}_{L/K}(f) = \sum_{i=1}^{r} \mathrm{Tr}_{\overline{k}((T_i))/\overline{k}((T))}(\alpha_i(f)). \tag{20}$$

Cette égalité est linéaire en f, et est vraie pour les générateurs de L/K ; elle est donc vraie pour tout $f \in L$.

Pour simplifier, notons $\mathrm{Tr}_i = \mathrm{Tr}_{\overline{k}((T_i))/\overline{k}((T))}$. Notons $\mathrm{Res}_T : \overline{k}((T)) \to \overline{k}$ l'application donnant le coefficient de T^{-1}. Pour montrer (19), il suffit d'après (20) d'établir

$$\mathrm{Res}_{P_i}(f\,dt) = \mathrm{Res}_T(\mathrm{Tr}_i(\alpha_i(f))) \qquad (f \in L). \tag{21}$$

Quitte à multiplier t_i par un scalaire non nul (les deux membres de (21) sont inchangés), on peut supposer $t = t_i^{e_i}(1 + a_1 t_i + a_2 t_i^2 + \cdots)$. Par récurrence, on obtient $t_i^{e_i} = h_0(t) + h_1(t)t_i + \cdots + h_{e_i-1}(t)t_i^{e_i-1}$, où les coefficients de $h_j \in \overline{k}((T))$ sont des polynômes à coefficients entiers en $a_1, a_2, \ldots$. Si $\alpha_i(f) = f_0 + f_1 T_i + \cdots + f_{e_i-1}T_i^{e_i-1}$ avec $f_j \in \overline{k}((T))$, alors $\mathrm{Res}_T(\mathrm{Tr}_i(\alpha_i(f)))$ est un polynôme à coefficients entiers en $a_1, a_2, \ldots$ et en les coefficients des f_j. Mais la même chose est vraie du membre de gauche de (21). Par le même principe que supra, il suffit donc de montrer (21) lorsque $\overline{k}$ est de caractéristique 0. Il existe $T_i' \in \overline{k}((T_i))$ telle que $(T_i')^{e_i} = T$ (prendre $T_i' = T_i \cdot (1 + a_1 T_i + \cdots)^{1/e_i}$). Alors tout élément de $\overline{k}((T_i))$ est une série formelle en T_i', et le résidu en P_i peut encore se calculer à l'aide de T_i', ce qui donne $\mathrm{Res}_{P_i}(f\,dt) = \mathrm{Res}_{T_i'}(\alpha_i(f) \cdot e_i T_i'^{e_i-1})$,

où $\mathrm{Res}_{T_i'}$ est le coefficient de $(T_i')^{-1}$. Posant $\alpha_i(f) = \sum_j \lambda_j T_i'^j$, il vient d'une part $\mathrm{Res}_{P_i}(f\,dt) = e_i\lambda_{-e_i}$ et d'autre part $\mathrm{Tr}_i(\alpha_i(f)) = e_i \sum_j \lambda_{je_i} T^j$, d'où (21) et le théorème 6.9. □

Posons $\widetilde{R} = \bigoplus_{P\in C} \overline{k}(C)$. L'espace R des *répartitions* est l'ensemble des $(f_P)_{P\in C} \in \widetilde{R}$ tels que $f_P \in \mathcal{O}_{C,P}$ sauf pour un nombre fini de P. C'est une $\overline{k}$-algèbre et on a une injection $j : \overline{k}(C) \to R$ qui à f associe la famille constante $(f)_{P\in C}$. Pour $P \in C$, soit j_P l'application qui à $f \in \overline{k}(C)$ associe la répartition égale à f en P, et nulle ailleurs. Pour tout diviseur $D \in \mathbf{Z}[C]$, posons

$$R(D) = \{(f_P)_{P\in C} \in R; \mathrm{ord}_P(f_P) \geq -\mathrm{ord}_P(D) \text{ pour tout } P \in C\}$$

et notons $I(D) = R/(R(D) + j(\overline{k}(C)))$. Si $D_1 \geq D_2$ alors $R(D_2) \subset R(D_1)$, d'où une application linéaire surjective $I(D_2) \to I(D_1)$. Pour tout diviseur $D \geq 0$, soit $\delta(D)$ la dimension du noyau de $I(0) \to I(D)$.

Lemme 6.10. — *Pour tout $D \geq 0$, les dimensions $\ell(D)$ et $\delta(D)$ sont finies et on a $\delta(D) = \deg D - \ell(D) + 1$.*

Démonstration. — Nous allons montrer ce résultat par récurrence. Si $D = 0$, le lemme affirme que $\ell(0) = 1$, ce qui découle du corollaire 2.37. Supposons le lemme est vrai pour D, et montrons-le pour $D + [P]$, où P est un point quelconque de C. On a $\delta(D + [P]) = \delta(D) + \varepsilon$ où ε est la dimension du noyau de $I(D) \to I(D + [P])$.

Pour tout $n \in \mathbf{Z}$, l'idéal fractionnaire $\mathfrak{m}_{C,P}^n$ de $\mathcal{O}_{C,P}$ est l'ensemble des $f \in \overline{k}(C)$ telles que $\mathrm{ord}_P(f) \geq n$. Posons $m = \mathrm{ord}_P(D)$ et $V = \mathfrak{m}_{C,P}^{-m-1}/\mathfrak{m}_{C,P}^{-m}$: c'est un $\overline{k}$-espace vectoriel de dimension 1. Nous allons montrer une suite exacte

$$0 \to \mathcal{L}(D) \to \mathcal{L}(D + [P]) \to V \to I(D) \to I(D + [P]) \to 0. \tag{22}$$

La première flèche est l'inclusion naturelle. La deuxième est la projection de $\mathcal{L}(D+[P]) \subset \mathfrak{m}_{C,P}^{-m-1}$ dans V. La troisième est induite par l'application j_P qui à $f \in \mathfrak{m}_{C,P}^{-m-1}$ associe la répartition égale à f au point P, et nulle ailleurs (on remarque que j_P envoie $\mathfrak{m}_{C,P}^{-m}$ dans $R(D)$, et $\mathfrak{m}_{C,P}^{-m-1}$ dans $R(D + [P])$). Enfin, la dernière flèche est la projection naturelle.

L'exactitude en $\mathcal{L}(D)$, $\mathcal{L}(D+[P])$, $I(D)$ et $I(D+[P])$ ne pose pas de problème. Montrons l'exactitude en V. Si $f \in \mathcal{L}(D+[P])$, on a $j_P(f) - j(f) \in R(D)$ et donc $j_P(f) \in R(D) + j(\overline{k}(C))$ est nul dans $I(D)$. Réciproquement, prenons $f \in \mathfrak{m}_{C,P}^{-m-1}$ telle que $j_P(f)$ est nul dans $I(D)$. Alors il existe $h \in \overline{k}(C)$ telle que $j_P(f) - j(h) \in R(D)$, ce qui entraîne $h \in \mathcal{L}(D+[P])$ et $f - h \in \mathfrak{m}_{C,P}^{-m}$, donc la classe de f dans V provient de $\mathcal{L}(D+[P])$.

On déduit de (22) que $\ell(D+[P])$ et ε sont finies et en prenant la suite alternée des dimensions, il vient $\ell(D) - \ell(D+[P]) + 1 - \epsilon = 0$, d'où la formule souhaitée pour $\delta(D+[P])$. □

Lemme 6.11. — *Pour tout $D \geq 0$, la dimension de $I(D)$ est finie.*

Démonstration. — Soit $f \in \overline{k}(C)$ une fonction non constante. Notons $\operatorname{div} f = D_0 - D_\infty$ où D_0 (resp. D_∞) est le diviseur des zéros (resp. pôles) de f. Notons n le degré de l'extension $\overline{k}(C)/\overline{k}(f)$. Soit B la fermeture intégrale de $\overline{k}[f]$ dans $\overline{k}(C)$. Soit $h_1, \ldots, h_n \in B$ une base de L/K. Nous avons vu dans la démonstration du théorème 2.35 que les pôles des h_i appartiennent à l'ensemble S des pôles de f. Par conséquent il existe N_0 tel que pour tout i, on ait $h_i \in \mathcal{L}(N_0 D_\infty)$. Pour $N \geq N_0$ et $0 \leq j \leq N - N_0$, on a $f^j h_i \in \mathcal{L}(N D_\infty)$ donc $\ell(N D_\infty) \geq (N - N_0 + 1)n$. Comme $\deg D_\infty = n$ d'après le théorème 2.35, il vient $\delta(N D_\infty) \leq (N_0 - 1)n + 1$ pour $N \geq N_0$. Il existe donc une constante M telle que $\delta(N D_\infty) \leq M$ pour tout $N \geq 0$.

Si $D \geq 0$ est quelconque, soit S' l'ensemble des $P \in C - S$ tels que $\operatorname{ord}_P(D) \geq 1$. Soit $m \geq 1$ et $h_m = \prod_{a \in S'} (f-a)^m \in \overline{k}[f]$. Pour N et m assez grands, on a $D \leq N D_\infty + \operatorname{div} h_m$ et donc $\delta(D) \leq \delta(N D_\infty + \operatorname{div} h_m)$. Or $\delta(N D_\infty + \operatorname{div} h_m) = \delta(N D_\infty)$ d'après le lemme 6.10. On en déduit que la fonction δ est bornée.

Soit $\widehat{D} \geq 0$ tel que $\delta(\widehat{D})$ est maximal. Soit $x \in R$. Il existe un diviseur D tel que $x \in R(D)$, et quitte à augmenter D on peut choisir $D \geq \widehat{D}$. Alors $I(\widehat{D}) \to I(D)$ est un isomorphisme par maximalité de $\delta(\widehat{D})$, ce qui signifie que $R(D) + \overline{k}(C) = R(\widehat{D}) + \overline{k}(C)$ et donc $\overline{x} = 0$ dans $I(\widehat{D})$. Il en résulte $I(\widehat{D}) = 0$. Par suite $I(0)$ est de dimension finie et c'est le cas aussi de $I(D)$ pour tout $D \geq 0$. □

Démonstration de Riemann-Roch. — Une utilisation répétée de la suite exacte (22) montre que $\ell(D)$ et $I(D)$ sont de dimension finie pour tout diviseur D. De plus, en notant $i(D)$ la dimension de $I(D)$, la somme alternée des dimensions donne $\ell(D+[P])-i(D+[P])=\ell(D)-i(D)+1$, ce qui entraîne que $\ell(D)-i(D)-\deg D$ est indépendant de D.

Pour terminer la preuve, on va montrer un cas particulier d'un théorème de dualité de Serre. Considérons la forme bilinéaire $\langle\cdot,\cdot\rangle : R\times\Omega^1(\overline{k}(C))\to\overline{k}$ donnée par $\langle(f_P)_{P\in C},\omega\rangle=\sum_{P\in C}\operatorname{Res}_P(f_P\omega)$, ce qui a un sens car la somme est en fait finie. Posons

$$\Omega(D)=\{\omega\in\Omega^1(\overline{k}(C))-\{0\};\operatorname{div}(\omega)\geq D\}\cup\{0\}.$$

Si $\omega_0\in\Omega^1(\overline{k}(C))-\{0\}$, on a $\Omega(D)=\mathcal{L}(\operatorname{div}\omega_0-D)\cdot\omega_0$ et donc $\Omega(D)$ est un $\overline{k}$-espace vectoriel de dimension $\ell(K_C-D)$.

Si $r=(f_P)_P\in R(D)$ et $\omega\in\Omega(D)$ alors $f_P\omega$ est régulière en P pour tout P, donc $\langle r,\omega\rangle=0$. De plus pour $f\in\overline{k}(C)$, on a $\langle j(f),\omega\rangle=0$ d'après le théorème 6.9 appliqué à $f\omega$. Donc $\langle\cdot,\cdot\rangle$ induit une forme $\overline{k}$-bilinéaire $I(D)\times\Omega(D)\to\overline{k}$. Montrons que cette forme bilinéaire est un accouplement parfait.

Soit $\omega\in\Omega(D)$ non nulle. Choisissons $P\in C$ et posons $n=\operatorname{ord}_P(\omega)$. Si $f\in\overline{k}(C)$ s'annule à l'ordre $-n-1$ en P, alors $\langle j_P(f),\omega\rangle\neq 0$. Ainsi l'application linéaire de $\Omega(D)$ dans le dual de $I(D)$ est injective.

Soit J l'ensemble des formes linéaires $\lambda : R\to\overline{k}$ pour lesquelles il existe un diviseur D tel que λ s'annule sur $R(D)+\overline{k}(C)$. L'espace J est muni d'une action de $\overline{k}(C)$: pour $f\in\overline{k}(C)$ et $\lambda\in J$, on pose $(f\cdot\lambda)(r)=\lambda(j(f)r)$. On a une application $\overline{k}(C)$-linéaire $\Omega^1(\overline{k}(C))\to J$ qui à ω associe $\langle\cdot,\omega\rangle$ (cette forme linéaire s'annnule sur $R(D)$ si $\omega\in\Omega(D)$). On vient de voir que cette application est injective. Pour montrer que c'est un isomorphisme, il suffit de montrer que $\dim_{\overline{k}(C)}J\leq 1$.

Supposons par l'absurde que $\lambda,\mu\in J$ sont linéairement indépendants sur $\overline{k}(C)$. Soit D un diviseur tel que λ et μ s'annulent sur $R(D)$. Si D' est un diviseur quelconque et $h\in\mathcal{L}(D')$, alors $h\lambda$ et $h\mu$ s'annulent sur $R(D+\operatorname{div}h)$ donc sur $R(D-D')$. Si $(h_1,\dots,h_r)$ est une base de $\mathcal{L}(D')$ alors $h_1\lambda,\dots,h_r\lambda,h_1\mu,\dots,h_r\mu$ sont linéairement indépendants sur $\overline{k}$ donc $2\ell(D')\leq i(D-D')$. En utilisant le fait que $\ell(D)-i(D)-\deg D$ est une constante M indépendante de D, il vient

$$2\deg D' + 2M \leq 2\ell(D') \leq i(D-D') \leq \ell(D-D') - \deg D + \deg D' - M$$

d'où une contradiction pour $\deg D'$ assez grand, car alors $\ell(D-D') = 0$.

Soit maintenant λ une forme linéaire sur $I(D)$. D'après ce qui précède, il existe $\omega \in \Omega^1(\overline{k}(C))$ telle que $\lambda(f) = \langle f, \omega\rangle$ pour toute $f \in R$. En prenant des répartitions bien choisies, on montre que $\omega \in \Omega(D)$. Ainsi $\langle\cdot,\cdot\rangle : I(D) \times \Omega(D) \to \overline{k}$ est parfait.

En particulier $i(D) = \dim \Omega(D) = \ell(K_C - D)$ pour tout diviseur D, et il vient $\ell(D) - \ell(K_C - D) - \deg D = \ell(D) - i(D) - \deg D = \ell(0) - i(0) = 1 - \dim\Omega(0) = 1 - g$, ce qui achève de démontrer Riemann-Roch. □

Démonstration de Riemann-Hurwitz. — L'application régulière $\phi : C \to C'$ induit, comme nous l'avons vu, un morphisme $\phi^* : \overline{k}(C') \to \overline{k}(C)$. En posant $\phi^*(f dg) = \phi^* f \cdot d\phi^*(g)$ pour $f, g \in \overline{k}(C')$ et en passant au quotient, on en déduit aussi une application $\overline{k}$-linéaire $\phi^* : \Omega^1(\overline{k}(C')) \to \Omega^1(\overline{k}(C))$ qui vérifie $\phi^*(f\omega) = \phi^*(f)\phi^*(\omega)$. Montrons que cette aplication est injective (nous allons ici utiliser la séparabilité de ϕ).

Soit t' une uniformisante en un point lisse de C'. D'après la proposition 2.40, dt' est une base de $\Omega^1(\overline{k}(C'))$. Il suffit donc de montrer que $\phi^*(dt') = d(\phi^* t') \neq 0$. Or l'extension $\overline{k}(\phi^* t') \subset \phi^*\overline{k}(C') \subset \overline{k}(C)$ est la composée d'extensions séparables, donc est séparable. Par le même argument que dans la démonstration de la proposition 2.40, on en déduit $d(\phi^* t) \neq 0$.

Soit maintenant $\omega \in \Omega^1(\overline{k}(C')) - \{0\}$. D'après le théorème de Riemann-Roch appliqué au diviseur $D = K_{C'}$, il vient $\ell(K_{C'}) - \ell(0) = \deg(K_{C'}) + 1 - g'$ et donc $\deg(K_{C'}) = \ell(K_{C'}) + g' - 2 = 2g' - 2$, où la dernière égalité vient de $\ell(K_{C'}) = \dim\Omega(0) = g'$ (on peut aussi utiliser Riemann-Roch avec $D = 0$). Par suite $\deg(\operatorname{div}\omega) = 2g' - 2$, et $\deg(\operatorname{div}\phi^*\omega) = 2g - 2$.

Il s'agit à présent de comparer les diviseurs de ω et $\phi^*\omega$. Soit $P \in C$, $Q = \phi(P)$ et $e = e_\phi(P)$. Soit t_P (resp. t_Q) une uniformisante en P (resp. Q), on a donc $\phi^* t_Q = t_P^e u$ avec $u \in \mathcal{O}^*_{C,P}$. Posant $\omega = f dt_Q$ avec $f \in \overline{k}(C')$, il vient $\phi^*\omega = \phi^* f \cdot d(\phi^* t_Q) = \phi^* f \cdot d(t_P^e u)$. Or

$$d(t_P^e u) = t_P^e du + e t_P^{e-1} u dt_P.$$

Comme u est régulière en P, on a $\operatorname{ord}_P(t_P^e du) \geq e$ d'après le lemme 2.42. De plus $\operatorname{ord}_P(e t_P^{e-1} u dt_P) \geq e-1$ avec égalité si e n'est pas divisible par la

caractéristique de k. On en déduit $\mathrm{ord}_P(\phi^*\omega) \geq \mathrm{ord}_P(\phi^* f) + e - 1$. Mais en posant $f = t_Q^{\mathrm{ord}_Q(f)} v$ avec $v \in \mathcal{O}_{C',Q}^*$, on a $\phi^* f = t_P^{e\,\mathrm{ord}_Q(f)} u^{\mathrm{ord}_Q(f)} \phi^* v$ d'où $\mathrm{ord}_P(\phi^* f) = e\,\mathrm{ord}_Q(f) = e\,\mathrm{ord}_Q(\omega)$. Finalement

$$\mathrm{ord}_P(\phi^*\omega) \geq e\,\mathrm{ord}_Q\,\omega + e - 1 \tag{23}$$

avec égalité si $\mathrm{car}(k) \nmid e$. En sommant sur $P \in C$, le degré du diviseur de $\phi^*\omega$ peut donc s'écrire

$$2g - 2 = \sum_{P \in C} \mathrm{ord}_P(\phi^*\omega) \geq \sum_{P \in C} e_\phi(P)\,\mathrm{ord}_{\phi(P)}(f) + e_\phi(P) - 1$$

Le membre de droite peut se réécrire

$$\sum_{Q \in C'} \Big(\sum_{\substack{P \in C \\ \phi(P) = Q}} e_\phi(P) \Big)\,\mathrm{ord}_Q(\omega) + \sum_{P \in C} e_\phi(P) - 1.$$

Remarquons que la dernière somme a un sens car $e_\phi(P) = 1$ sauf pour un nombre fini de P, d'après l'inégalité (23). Le résultat découle alors du théorème 2.51. □

Références

[1] C. Bavard – « La surface de Klein », *Le journal de maths des élèves* **1** (1993), p. 13–22, `http://www.umpa.ens-lyon.fr/JME/Vol1Num1/artCBavard/artCBavard.html`.

[2] J.-P. Serre – *Groupes algébriques et corps de classes*, 2de éd., Publications de l'Institut mathématique de l'université de Nancago, 7, Hermann, Paris, 1984, Actualités scientifiques et industrielles, 1264.

[3] J. H. Silverman – *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1994, Corrected reprint of the 1986 original.

Version du 24 avril 2009

François Brunault • *E-mail :* `brunault@umpa.ens-lyon.fr`, ÉNS Lyon, UMPA, 46 allée d'Italie, 69007 Lyon, France